Configuring IP Multicasting Services

Router Software Version 11.02
Site Manager Software Version 5.02

Part No. 114064 Rev. B
May 1997

Bay Networks

Bay Networks

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

Copyright © 1988–1997 Bay Networks, Inc.

All rights reserved. Printed in the USA. May 1997.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Bay Networks, Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. A summary of the Software License is included in this document.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notice for All Other Executive Agencies

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Trademarks of Bay Networks, Inc.

ACE, AFN, AN, BCN, BLN, BN, BNX, CN, FN, FRE, GAME, LN, Optivity, PPX, Bay Networks, SynOptics, SynOptics Communications, Wellfleet and the Wellfleet logo are registered trademarks and Advanced Remote Node, ANH, ARN, ASN, Bay•SIS, BayStack, BayStream, BCNX, BLNX, EZ Install, EZ Internetwork, EZ LAN, IP AutoLearn, PathMan, PhonePlus, Quick2Config, RouterMan, SN, SPEX, Switch Node, Bay Networks Press, the Bay Networks logo and the SynOptics logo are trademarks of Bay Networks, Inc.

Third-Party Trademarks

All other trademarks and registered trademarks are the property of their respective owners.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Bay Networks, Inc. reserves the right to make changes to the products described in this document without notice.

Bay Networks, Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product are Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

USA Requirements Only

Federal Communications Commission (FCC) Compliance Notice: Radio Frequency Notice

This equipment generates, uses, and can radiate radio-frequency energy. If you do not install and use this equipment according to the instruction manual, this product may interfere with radio communications. This product has been tested and found to comply with the limits for a Class A computing device, pursuant to Subpart J of Part 15 of FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. Operating this equipment in a residential area is likely to interfere with radio communications; in which case, the user, at his/her own expense, must correct the interference.

Shielded-compliant cables must be used with this unit to ensure compliance with the Class A limits.

EN 55 022 Declaration of Conformance

This is to certify that the Bay Networks products in this book are shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55 022:1987 Class A (CISPR 22:1985/BS 6527:1988).

EN 55 022 Declaration of Conformance

This is to certify that the Bay Networks products in this book are shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55 022:1987 Class B (CISPR 22:1985/BS 6527:1988).

Japan/Nippon Requirements Only

Voluntary Control Council for Interference (VCCI) Statement

この装置は、第一種情報装置（商工業地域において使用されるべき情報装置）で、商工業地域での電波障害防止を目的とした情報処理装置等電波障害自主規制協議会（VCCI）基準に適合しております。

従って、住宅地域、その隣接地域等で使用した場合、ラジオ、テレビ受信機等に障害を与えることがあります。

上記基準に適合する遮蔽ケーブルをご自分でお求めになり、取扱説明書に従って、正しくご使用ください。

Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the 1st category (information equipment to be used in commercial and/or industrial areas) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines that are aimed at preventing radio interference in commercial and/or industrial areas.

Consequently, when this equipment is used in a residential area or in an adjacent area thereto, radio interference may be caused to equipment such as radios and TV receivers.

Compliance with the applicable regulations is dependent upon the use of shielded cables. The user is responsible for procuring the appropriate cables. Read instructions for correct handling.

Canada Requirements Only

Canada CS-03 Rules and Regulations

Note: The Canadian Department of Communications label identifies certified equipment. The certification means that the equipment meets certain telecommunications network protective operations and safety requirements. The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single line individual service may be extended by means of a certified connector assembly (telephone extension cord). The customer should be aware that compliance with the above conditions may not prevent the degradation of service in some situations.

Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

Canada CS-03 -- Règles et règlements

Note: L’étiquette du ministère des Communications du Canada indique que l’appareillage est certifié, c’est-à-dire qu’il respecte certaines exigences de sécurité et de fonctionnement visant les réseaux de télécommunications. Le ministère ne garantit pas que l’appareillage fonctionnera à la satisfaction de l’utilisateur.

Avant d’installer l’appareillage, s’assurer qu’il peut être branché aux installations du service de télécommunications local. L’appareillage doit aussi être raccordé selon des méthodes acceptées. Dans certains cas, le câblage interne du service de télécommunications utilisé pour une ligne individuelle peut être allongé au moyen d’un connecteur certifié (prolongateur téléphonique). Le client doit toutefois prendre note qu’une telle installation n’assure pas un service parfait en tout temps.

Les réparations de l’appareillage certifié devraient être confiées à un service d’entretien canadien désigné par le fournisseur. En cas de réparation ou de modification effectuées par l’utilisateur ou de mauvais fonctionnement de l’appareillage, le service de télécommunications peut demander le débranchement de l’appareillage.

Pour leur propre sécurité, les utilisateurs devraient s’assurer que les mises à la terre des lignes de distribution d’électricité, des lignes téléphoniques et de la tuyauterie métallique interne sont raccordées ensemble. Cette mesure de sécurité est particulièrement importante en milieu rural.

Attention: Les utilisateurs ne doivent pas procéder à ces raccordements eux-mêmes mais doivent plutôt faire appel aux pouvoirs de réglementation en cause ou à un électricien, selon le cas.

Canada Requirements Only *(continued)*

D. O. C. Explanatory Notes: Equipment Attachment Limitations

The Canadian Department of Communications label identifies certified equipment. This certification meets certain telecommunication network protective, operational and safety requirements. The department does not guarantee the equipment will operate to the users satisfaction.

Before installing the equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single line individual service may be extended by means of a certified connector assembly (telephone extension cord). The customer should be aware that compliance with the above condition may not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution: Users should not attempt to make such connections themselves, but should contact the appropriate electrical inspection authority, or electrician, as appropriate.

Notes explicatives du ministère des Communications: limites visant les accessoires

L'étiquette du ministère des Communications du Canada indique que l'appareillage est certifié, c'est-à-dire qu'il respecte certaines exigences de sécurité et de fonctionnement visant les réseaux de télécommunications. Le ministère ne garantit pas que l'appareillage fonctionnera à la satisfaction de l'utilisateur.

Avant d'installer l'appareillage, s'assurer qu'il peut être branché aux installations du service de télécommunications local. L'appareillage doit aussi être raccordé selon des méthodes acceptées. Dans certains cas, le câblage interne du service de télécommunications utilisé pour une ligne individuelle peut être allongé au moyen d'un connecteur certifié (prolongateur téléphonique). Le client doit toutefois prendre note qu'une telle installation n'assure pas un service parfait en tout temps.

Les réparations de l'appareillage certifié devraient être confiées à un service d'entretien canadien désigné par le fournisseur. En cas de réparation ou de modification effectuées par l'utilisateur ou de mauvais fonctionnement de l'appareillage, le service de télécommunications peut demander le débranchement de l'appareillage.

Pour leur propre sécurité, les utilisateurs devraient s'assurer que les mises à la terre des lignes de distribution d'électricité, des lignes téléphoniques et de la tuyauterie métallique interne sont raccordées ensemble. Cette mesure de sécurité est particulièrement importante en milieu rural.

Attention: Les utilisateurs ne doivent pas procéder à ces raccordements eux-mêmes mais doivent plutôt faire appel aux pouvoirs de réglementation en cause ou à un électricien, selon le cas.

Canada Requirements Only *(continued)*

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (Access Feeder Node, Access Link Node, Access Node, Access Stack Node, Advanced Remote Node, Backbone Concentrator Node, Backbone Concentrator Node Switch, Backbone Link Node, Backbone Link Node Switch, Concentrator Node, Feeder Node, Link Node, Switch Node) does not exceed the Class A limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

Règlement sur le brouillage radioélectrique du ministère des Communications

Cet appareil numérique (Access Feeder Node, Access Link Node, Access Node, Access Stack Node, Advanced Remote Node, Backbone Concentrator Node, Backbone Concentrator Node Switch, Backbone Link Node, Backbone Link Node Switch, Concentrator Node, Feeder Node, Link Node, Switch Node) respecte les limites de bruits radioélectriques visant les appareils numériques de classe A prescrites dans le Règlement sur le brouillage radioélectrique du ministère des Communications du Canada.

T1 Service Compliance Statements

T1 Service

NOTE: This T1 Service notice applies to you only if you have received a single or dual port Multi-Channel T1 (MCT1) Link Module (which provides an internal CSU).

This equipment complies with Part 68 of FCC Rules. Please note the following:

1. You are required to request T1 service from the telephone company before you connect the CSU to a T1 network. When you request T1 service, you must provide the telephone company with the following data:
   - The Facility Interface Code

     Provide the telephone company with both codes below:

     — 04DU9-B (1.544 MB D4 framing format)
     — 04DU9-C (1.544 MB ESF format)

     The telephone company will select the code it has available.
   - The Service Order Code: 6.0F
   - The required USOC jack: RJ48C
   - The make, model number, and FCC Registration number of the CSU.
2. Your telephone company may make changes to its facilities, equipment, operations, or procedures that could affect the proper functioning of your equipment. The telephone company will notify you in advance of such changes to give you an opportunity to maintain uninterrupted telephone service.
3. If your CSU causes harm to the telephone network, the telephone company may temporarily discontinue your service. If possible, they will notify you in advance, but if advance notice is not practical, you will be notified as soon as possible and will be informed of your right to file a complaint with the FCC.
4. If you experience trouble with the CSU, please contact Bay Networks Technical Response Center in your area for service or repairs. Repairs should be performed only by service personnel authorized by Bay Networks, Inc.

United States	1-800-2LAN-WAN
Valbonne, France	(33) 92-968-968
Sydney, Australia	(612) 9927-8800
Tokyo, Japan	(81) 3-5402-0180
5. You are required to notify the telephone company when you disconnect the CSU from the network and when you disconnect the BCNX or BLNX from the network.

Bay Networks Software License

Note: This is Bay Networks basic license document. In the absence of a software license agreement specifying varying terms, this license -- or the license included with the particular product -- shall govern licensee's use of Bay Networks software.

This Software License shall govern the licensing of all software provided to licensee by Bay Networks ("Software"). Bay Networks will provide licensee with Software in machine-readable form and related documentation ("Documentation"). The Software provided under this license is proprietary to Bay Networks and to third parties from whom Bay Networks has acquired license rights. Bay Networks will not grant any Software license whatsoever, either explicitly or implicitly, except by acceptance of an order for either Software or for a Bay Networks product ("Equipment") that is packaged with Software. Each such license is subject to the following restrictions:

1. Upon delivery of the Software, Bay Networks grants to licensee a personal, nontransferable, nonexclusive license to use the Software with the Equipment with which or for which it was originally acquired, including use at any of licensee's facilities to which the Equipment may be transferred, for the useful life of the Equipment unless earlier terminated by default or cancellation. Use of the Software shall be limited to such Equipment and to such facility. Software which is licensed for use on hardware not offered by Bay Networks is not subject to restricted use on any Equipment, however, unless otherwise specified on the Documentation, each licensed copy of such Software may only be installed on one hardware item at any time.
2. Licensee may use the Software with backup Equipment only if the Equipment with which or for which it was acquired is inoperative.
3. Licensee may make a single copy of the Software (but not firmware) for safekeeping (archives) or backup purposes.
4. Licensee may modify Software (but not firmware), or combine it with other software, subject to the provision that those portions of the resulting software which incorporate Software are subject to the restrictions of this license. Licensee shall not make the resulting software available for use by any third party.
5. Neither title nor ownership to Software passes to licensee.
6. Licensee shall not provide, or otherwise make available, any Software, in whole or in part, in any form, to any third party. Third parties do not include consultants, subcontractors, or agents of licensee who have licensee's permission to use the Software at licensee's facility, and who have agreed in writing to use the Software only in accordance with the restrictions of this license.
7. Third-party owners from whom Bay Networks has acquired license rights to software that is incorporated into Bay Networks products shall have the right to enforce the provisions of this license against licensee.
8. Licensee shall not remove or obscure any copyright, patent, trademark, trade secret, or similar intellectual property or restricted rights notice within or affixed to any Software and shall reproduce and affix such notice on any backup copy of Software or copies of software resulting from modification or combination performed by licensee as permitted by this license.

9. Licensee shall not reverse assemble, reverse compile, or in any way reverse engineer the Software. [Note: For licensees in the European Community, the Software Directive dated 14 May 1991 (as may be amended from time to time) shall apply for interoperability purposes. Licensee must notify Bay Networks in writing of any such intended examination of the Software and Bay Networks may provide review and assistance.]
10. Notwithstanding any foregoing terms to the contrary, if licensee licenses the Bay Networks product "Site Manager," licensee may duplicate and install the Site Manager product as specified in the Documentation. This right is granted solely as necessary for use of Site Manager on hardware installed with licensee's network.
11. This license will automatically terminate upon improper handling of Software, such as by disclosure, or Bay Networks may terminate this license by written notice to licensee if licensee fails to comply with any of the material provisions of this license and fails to cure such failure within thirty (30) days after the receipt of written notice from Bay Networks. Upon termination of this license, licensee shall discontinue all use of the Software and return the Software and Documentation, including all copies, to Bay Networks.
12. Licensee's obligations under this license shall survive expiration or termination of this license.

Contents

About This Guide

Before You Begin xxi
Conventions xxii
Acronyms xxiii
Ordering Bay Networks Publications xxiv
Bay Networks Customer Service xxiv
How to Get Help xxv
For More Information xxv

Chapter 1
Multicasting Overview

Multicast Host Groups 1-1
Multicast Addresses 1-2
Multicast Protocols 1-3
Group Membership Protocols 1-3
Routing Protocols 1-3

Chapter 2
Starting IP Multicasting Services

Starting IGMP and DVMRP 2-1
Starting ST2 2-3

Chapter 3
Customizing IGMP

IGMP Concepts and Terminology 3-2
IGMP Queries 3-2
IGMP Host Reports 3-2
Host Leave Messages 3-3

Configuring IGMP on the Router 3-3
Enabling and Disabling IGMP 3-3
Estimating the Number of Groups 3-4
Specifying a Version Threshold Time 3-4
Configuring Logging 3-4
Configuring IGMP on an Interface 3-5
Enabling and Disabling IGMP 3-5
Specifying a Query Rate 3-5
Specifying a Membership Timeout Interval 3-6
Specifying a Designated Router Timeout Interval 3-6
Specifying a Maximum Host Response Time 3-6
Configuring a Static Host Entry 3-7

Chapter 4
Customizing DVMRP

DVMRP Concepts and Terminology 4-2
Neighbor Connections 4-2
Source Route Advertisements 4-4
How DVMRP Chooses a Route 4-4
Routing Table and Forwarding Table 4-5
Shortest-Path Trees 4-6
Configuring DVMRP on the Router 4-7
Setting the Update Interval 4-7
Configuring Tree Pruning 4-8
Configuring DVMRP Timers 4-9
Setting the Route Expiration Timer 4-9
Setting the Garbage Timer 4-9
Setting the Neighbor Report Timer 4-10
Setting the Leaf Timer 4-10
Specifying a Probe Interval 4-11
Specifying a Route Switch Interval 4-11
Estimating the Number of Routes 4-11
Logging Debugging Messages 4-12
Specifying an MTU Size 4-12
Specifying the Maximum Number of Routes 4-12

Configuring DVMRP on a Circuit 4-13
Enabling and Disabling DVMRP 4-13
Disabling Multicast Support 4-13
Calculating a Route Metric and Comparing Route Costs 4-13
Specifying a Threshold 4-14
Configuring a Forwarding Table 4-15
Disabling Advertisement of Local Networks 4-16
Configuring a Tunnel 4-16
Enabling and Disabling the Tunnel 4-16
Selecting the Encapsulation Mode 4-16
Specifying the Cost 4-17
Specifying a TTL 4-17
Configuring a Forwarding Table for the Tunnel 4-17
Supplying Addresses for the Tunnel 4-18

Chapter 5
Customizing ST2 Services

ST2 Concepts and Terminology 5-2
ST2 and IP 5-2
ST2 Agents 5-2
Stream Control Messages 5-4
Neighbors and Tunnels 5-4
Resource Manager 5-5
ST2 Features 5-6
The Role of an ST2 Intermediate Agent 5-7
How the Agent Sets Up a Stream Segment 5-7
Receiving a Connect Request from Upstream 5-7
Determining the Next Hop Downstream 5-9
Using the IP Routing Table (IP-Inherited Routing) 5-9
Using the ST2 Neighbor Table (Exploratory Routing) 5-10
Establishing a Connection with a Downstream Neighbor 5-10
How the Agent Adds a Target to a Stream 5-10
How the Agent Forwards ST2 Data Downstream 5-12
How the Agent Shuts Down a Stream 5-12

Configuring ST2 on the Router 5-12
Enabling and Disabling ST2 5-12
Configuring the Tunnel Capability 5-13
Configuring an ST2 Interface 5-13
Enabling and Disabling ST2 5-13
Specifying an IP Address 5-13
Setting Interface Timers and Counters 5-14
Configuring the Neighbors Forwarding Table 5-15

Chapter 6
Reserving Line Resources

About Line Resource Reservation 6-2
Resource Manager 6-2
Supported Media 6-2
How the Resource Manager Works with ST2 6-3
Starting the Resource Manager 6-3
Configuring the Resource Manager 6-6
Setting the Estimated Bandwidth 6-7
Setting the Reservable Bandwidth 6-7
Specifying the Traffic Queuing Algorithm 6-7
Specifying the Policing Algorithm 6-8
Setting the Bandwidth Interval 6-8
Setting the Inflate Reservations Percentage 6-9
Specifying the Unreserved Policing Algorithm 6-9
Specifying the Unreserved Queue Length 6-10
Specifying the Multiline Select Algorithm 6-10
Setting the Multiline Threshold Bandwidth 6-10
Setting the Reservation Latency 6-11
Disabling Line Resource Management 6-12
Removing a Line's Reservations 6-12
Deleting Resource Manager Services 6-12

Appendix A
Site Manager Multicast Parameters

DVMRP Parameters A-1
DVMRP Global Parameters A-2
DVMRP Circuit Parameters A-7
DVMRP Tunnel Parameters A-10
IGMP Parameters A-12
IGMP Global Configuration Parameters A-13
IGMP Static Host Parameters A-14
IGMP Entry Interface Parameters A-15
IP Configuration Parameters A-17
ST2 Parameters A-19
ST2 Global Parameters A-19
ST2 Interface Parameters A-20
ST2 Neighbors Forwarding Table Parameters A-24
Resource Manager Parameters A-27

Index

Figures

Figure 4-1. Multicast Routers 4-3
Figure 5-1. ST2 Point-to-Multipoint Stream 5-3
Figure 5-2. ST2 Neighbors 5-5
Figure 5-3. Setting Up a Point-to-Point Stream 5-8
Figure 5-4. Adding a Target to a Stream 5-11
Figure 6-1. MCT1 Logical Lines Window 6-4
Figure 6-2. Edit Connector Window 6-4
Figure 6-3. Creating the Line Resources Record 6-5
Figure 6-4. Edit Line Resources Window 6-5
Figure 6-5. Removing a Line's Reserved Resources 6-12
Figure 6-6. Deleting the Circuit's Resource Manager (CRM) 6-13

Tables

Table 4-1. Routing Table Entry Items 4-5
Table 4-2. Forwarding Table Entry Items 4-6
Table 4-3. Recommended TTL and Threshold Values 4-15
Table 5-1. ST2 Features 5-6
Table 5-2. ST2 Timers 5-14

About This Guide

If you are responsible for configuring and managing Bay Networks® routers, you need to read this guide.

If you want to	Go to
Learn about multicasting concepts and terminology	Chapter 1
Start IGMP, DVMRP, or ST2	Chapter 2
Customize IGMP	Chapter 3
Customize DVMRP	Chapter 4
Customize ST2	Chapter 5
Reserve ST2 line resources	Chapter 6
Configure Site Manager multicast parameters	Appendix A

Before You Begin

Before using this guide, you must complete the following procedures. For a new router:

- Install the router (refer to the installation manual that came with your router).
- Connect the router to the network and create a pilot configuration file (refer to *Quick-Starting Routers and BayStream Platforms* or *Configuring Remote Access)*.

Make sure that you are running the latest version of Bay Networks Site Manager and router software. For instructions, refer to *Upgrading Routers from Version 7–10.xx to Version 11.0*.

Conventions

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: if command syntax is **ping** *<ip_address>*, you enter **ping 192.32.10.12**
bold text	Indicates text that you need to enter, command names, and buttons in menu paths. Example: Enter **wfsm &**
	Example: Use the **dinfo** command.
	Example: ATM DXI > Interfaces > **PVCs** identifies the PVCs button in the window that appears when you select the Interfaces option from the ATM DXI menu.
brackets ([ ])	Indicate optional elements. You can choose none, one, or all of the options.
ellipsis points	Horizontal (. . .) and vertical (⋮) ellipsis points indicate omitted information.
italic text	Indicates variable values in command syntax descriptions, new terms, file and directory names, and book titles.
quotation marks (“ ”)	Indicate the title of a chapter or section within a book.
`screen text`	Indicates data that appears on the screen. Example: `Set Bay Networks Trap Monitor Filters`
separator (>)	Separates menu and option names in instructions and internal pin-to-pin wire connections. Example: Protocols > AppleTalk identifies the AppleTalk option in the Protocols menu.
	Example: Pin 7 > 19 > 20
vertical line (|)	Indicates that you enter only one of the parts of the command. The vertical line separates choices. Do not type the vertical line when entering the command. Example: If the command syntax is
	show at routes | **nets**, you enter either **show at routes** or **show at nets**, but not both.

Acronyms

AUI	Attachment Unit Interface
BOOTP	Bootstrap Protocol
BRI	Basic Rate Interface
CCITT	International Telegraph and Telephone Consultative Committee (now ITU-T)
CSMA/CD	carrier sense multiple access with collision detection
DLCMI	Data Link Control Management Interface
GUI	graphical user interface
HDLC	high-level data link control
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ITU-T	International Telecommunications Union–Telecommunications (formerly CCITT)
LAN	local area network
MAC	media access control
MAU	media access unit
MDI-X	media-dependent interface with crossover
NBMA	nonbroadcast multi-access
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First (Protocol)
PPP	Point-to-Point Protocol
RIP	Routing Information Protocol
SMDS	switched multimegabit data service
SNMP	Simple Network Management Protocol
STP	shielded twisted-pair
TCP/IP	Transmission Control Protocol/Internet Protocol
TELNET	Telecommunication Network
TFTP	Trivial File Transfer Protocol
TPE	twisted-pair Ethernet
UTP	unshielded twisted-pair
WAN	wide area network

Ordering Bay Networks Publications

To purchase additional copies of this document or other Bay Networks publications, order by part number from Bay Networks Press™ at the following numbers:

- Phone--U.S./Canada: 1-888-422-9773
- Phone--International: 1-510-490-4752
- FAX--U.S./Canada and International: 1-510-498-2609

Bay Networks Customer Service

You can purchase a support contract from your Bay Networks distributor or authorized reseller, or directly from Bay Networks Services. For information about, or to purchase a Bay Networks service contract, either call your local Bay Networks field sales office or one of the following numbers:

Region	Telephone number	Fax number
United States and Canada	1-800-2LANWAN; then enter Express Routing Code (ERC) 290, when prompted, to purchase or renew a service contract 1-508-916-8880 (direct)	1-508-670-8766
Europe	33-4-92-96-69-66	33-4-92-96-69-96
Asia/Pacific	61-2-9927-8888	61-2-9927-8899
Latin America	561-988-7661	561-988-7550

How to Get Help

If you purchased a service contract for your Bay Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Bay Networks service program, call one of the following Bay Networks Technical Support Centers:

Technical Support Center	Telephone number	Fax number
Billerica, MA	1-800-2LANWAN	508-670-8765
Santa Clara, CA	1-800-2LANWAN	408-495-1188
Valbonne, France	33-4-92-96-69-68	33-4-92-96-69-98
Sydney, Australia	61-2-9927-8800	61-2-9927-8811
Tokyo, Japan	81-3-5402-0180	81-3-5402-0173

For More Information

For information about Bay Networks and its products, visit the Bay Networks World Wide Web (WWW) site at http://www.baynetworks.com. To learn more about Bay Networks Customer Service, select Customer Service on the opening Web page.

Chapter 1
Multicasting Overview

The following sections describe IP multicasting concepts and terminology:

- Multicast Host Groups -- page 1-1
- Multicast Addresses -- page 1-2
- Multicast Protocols -- page 1-3

  Group Membership Protocols -- page 1-3
  Routing Protocols -- page 1-3

Multicast Host Groups

IP multicasting is a method for addressing, routing, and delivering a datagram to a collection of receivers called a *host group*.

Host groups can be permanent or transient:

- A *permanent host group* has a well-known, administratively assigned IP multicast group address. The address, not the membership, is permanent and defines the group. A permanent host group can consist of zero or more members.
- A *transient host group* exists only as long as it has members that need its services. IP addresses in the multicast range that are not reserved for permanent groups are available for dynamic assignment to transient host groups.

Any host system on any IP network can send a message to a multicast group using the group's IP multicast address. To receive a message addressed to a multicast group, however, the host must be a member of the group and must reside on a network where that group is registered with a local multicast router.

An IP multicasting host group can consist of zero or more members and places no restrictions on its membership. Host members can reside anywhere; they can join and leave the group at any time; and they can be members of more than one group at the same time. In order to receive a multicast message from a host group, a host must be a member of the group. However, anyone can send a multicast datagram: a host does not need to be a member of a group to send a multicast message to its members.

In general, hosts that are members of the same group reside on different networks. However, a range of multicast addresses (224.0.0.*x*) is reserved for groups that are locally scoped. All message traffic for these hosts remains on the local network. Hosts that belong to a group in this address range and that reside in different networks will not receive each other's message traffic.

Note: Multicast data packets are affected by traffic filters. The network administrator must ensure that traffic filters configured on a multicast router do not prevent a host that is a member of a group from receiving packets intended for that group.

Multicast Addresses

Each host group is assigned a unique multicast address. To reach all members of the group, a sender uses the multicast address as the destination address of the datagram.

An IP Version 4 multicast address is a Class D address (the high-order bits are set to 1110) in the range of 224.0.0.0 to 239.255.255.255.

The block of addresses from 224.0.0.1 to 224.0.0.255 is reserved for routing protocols and other low-level protocols. Multicast routers will not forward datagrams with addresses in this range.

Multicast Protocols

An IP router fully configured for multicasting runs a host group membership protocol and a multicast routing protocol.

Group Membership Protocols

A *group membership protocol* allows a router to learn the existence of group members on its directly attached networks. The router periodically sends a group query to each of its local networks. Any host that is a member of a multicasting group identifies itself by responding.

Bay Networks implements the Internet Group Management Protocol (IGMP), which is described in Chapter 3.

Routing Protocols

A *multicast routing protocol* defines data paths that enable routers to forward multicast datagrams from a single source to multiple destinations.

There are two types of IP routing protocols:

- A *dense-mode* routing protocol is designed to support groups whose members are located in a single internet region.

  Bay Networks currently implements one IP dense-mode routing protocol, DVMRP (Distance Vector Multicast Routing Protocol). DVMRP is described in Chapter 4.

- A *sparse-mode* routing protocol is designed to support groups whose members are located in multiple internet regions.

Note that the terms “dense” and “sparse” refer to the distribution of members in a group -- not to the number of members in the group.

Chapter 2
Starting IP Multicasting Services

The following sections explain how to configure IP multicast services using all available defaults:

- Starting IGMP and DVMRP -- page 2-1
- Starting ST2 -- page 2-3

Starting IGMP and DVMRP

This section shows you how to start IGMP and DVMRP using all default values and settings. For information on modifying the defaults, see Chapters 3 and 4.

Before you can select a protocol to run on a router, you must configure a circuit that the protocol can use as an interface to an attached network. For information and instructions, see *Configuring WAN Line Services*.

When you have successfully configured the circuit, the Select Protocols window opens.

1. **In the Select Protocols window, select IP, IGMP, and DVMRP and click on OK.**

   The IP Configuration window opens.

2. **Supply the following information:**

   - *An IP address for this interface.* There is no default for the IP address. You must supply an address or enter 0.0.0.0 to indicate that this is an unnumbered interface. (For information about unnumbered interfaces, see *Configuring IP Services*.)

     Site Manager: IP Address parameter: page A-17

   - *A subnet mask.* When you specify an address, IP automatically calculates an appropriate subnet mask, depending on the class of network. You can use Site Manager to override the default mask.

     Site Manager: Subnet Mask parameter: page A-17

   - *A transmit broadcast address*. By default, IP uses a broadcast address that consists of all 1s. You can use Site Manager to override the default.

     Site Manager: Transmit Bcast Addr parameter: page A-18

   - *An associated IP address.* If you are configuring an unnumbered IP interface, use Site Manager to supply an associated IP address.

     Site Manager: UnNumbered Assoc Address parameter: page A-18

3. **Click on OK.**

   The Initial IGMP Global Parameters window opens.

4. **Click on Save to accept the default parameters.**

   The Initial DVMRP Base Parameters window opens.

5. **Click on Save to accept the default parameters.**

Starting ST2

This section shows you how to start ST2 using all default values and settings. For information on modifying ST2 defaults, see Chapter 5

Before you can select a protocol to run on a router, you must configure a circuit that the protocol can use as an interface to an attached network. For information and instructions, see *Configuring WAN Line Services*.

When you have successfully configured the circuit, the Select Protocols window opens.

1. **In the Select Protocols window, select IP and ST2 and click on OK.**

   The IP configuration window opens.

2. **Supply the following information:**

   - *An IP address for this interface.* There is no default for the IP address. You must supply an address or enter 0.0.0.0 to indicate that this is an unnumbered interface. (For information about unnumbered interfaces, see *Configuring IP Services*.)

     Site Manager: IP Address parameter: page A-17

   - *A subnet mask.* When you specify an address, IP automatically calculates an appropriate subnet mask, depending on the class of network. You can use Site Manager to override the default mask.

     Site Manager: Subnet Mask parameter: page A-17

   - *A transmit broadcast address*. By default, IP uses a broadcast address that consists of all 1s. You can use Site Manager to override the default.

     Site Manager: Transmit Bcast Addr parameter: page A-18

- *An associated IP address.* If you are configuring an unnumbered IP interface, use Site Manager to supply an associated IP address.

Site Manager: UnNumbered Assoc Address parameter: page A-18

3. **Click on OK.**

Chapter 3
Customizing IGMP

This chapter consists of the following sections describing the Internet Group Management Protocol (IGMP):

- IGMP Concepts and Terminology -- page 3-2
  - IGMP Queries -- page 3-2
  - IGMP Host Reports -- page 3-2
  - Host Leave Messages -- page 3-3
- Configuring IGMP on the Router -- page 3-3
  - Estimating the Number of Groups -- page 3-4
  - Specifying a Version Threshold Time -- page 3-4
  - Configuring Logging -- page 3-4
- Configuring IGMP on an Interface -- page 3-5
  - Specifying a Query Rate -- page 3-5
  - Specifying a Membership Timeout Interval -- page 3-6
  - Specifying a Designated Router Timeout Interval -- page 3-6
  - Specifying a Maximum Host Response Time -- page 3-6
- Configuring a Static Host Entry -- page 3-7

IGMP Concepts and Terminology

The IGMP allows a host to register its local network with the local router to receive any datagrams sent to this router and targeted to a group with a specific IP multicast address. Bay Networks routers support IGMP Version 2.

A router communicates with the hosts on a local network by sending IGMP queries. Hosts respond by issuing IGMP reports.

IGMP Queries

A router running IGMP periodically sends host membership queries to its attached local networks. Routers that conform to RFC 1112 generate Version 1 queries. Bay Networks routers configured with IGMP generate Version 2 queries.

If multiple IGMP routers exist on the network, routers designate one router to send host member questions, using the following rules:

- Choose a router that generates Version 1 queries over a router that generates Version 2 queries.
- Choose the router with the lowest IP address.

IGMP Host Reports

A host that receives a membership query from a local router can respond with a *host membership report*, one report for each supported multicast group. A host that receives a query delays its reply by a random interval and listens for a reply from any other host in the same host group. Consider a network that includes two host members -- Host A and Host B -- of the same multicast group. The router sends out a host membership query on the local network. Host A and Host B both receive the query and listen on the network for a host membership report. Host B's delay time expires first, so it responds to the query with a membership report. Hearing the response, Host A does not send a report of its own for the same group.

Each query from a router to a host includes a code field. IGMP inserts a value (*d*) into this field specifying the maximum time in tenths of a second within which the host must issue a reply. The host uses this value to calculate a random value between 0 and *d* tenths of a second for the period that it waits before sending a response.

If at least one host on the local network specifies that it is a member of a given group, the router will forward to that network all datagrams bearing the group's multicast address.

Host Leave Messages

When a Version 2 host leaves a group, it issues a *Host Leave message*. The multicast router on the network issues a host query to determine whether there are other group members on the network. If no host responds to the query, the router assumes that no members belonging to that group exist on that interface.

Upon initialization, the host may immediately issue a report for each of its supported multicast groups. The router accepts and processes these asynchronous reports the same way it accepts requested reports.

Once in a steady state, hosts and routers communicate in a way that minimizes the exchange of queries and reports.

Configuring IGMP on the Router

The following sections show you how to configure IGMP features on the router using Site Manager.

Enabling and Disabling IGMP

IGMP is automatically enabled when you configure it on a router.You can use Site Manager to disable and reenable IGMP.

Site Manager: Enable parameter: page A-13

Estimating the Number of Groups

By default, IGMP estimates that 20 groups will be simultaneously active on a router. You can use Site Manager to supply an estimate from 5 to 65,535 groups.

Site Manager: Estimated Groups parameter: page A-13

This estimate allows the router to utilize memory efficiently. Exceeding this size during router operation will not cause an error, but may cause the router to consume more memory than required.

Note: The following groups are not maintained by IGMP; you do not need to include them in the count: 224.0.0.1, 224.0.0.4, 224.0.0.5, and 224.0.0.6.

Specifying a Version Threshold Time

By default, 540 seconds can elapse after IGMP detects a Version 1 query and before it tries to become the designated querier. You can use Site Manager to specify a version threshold time from 1 to 65535 seconds.

Site Manager: Version Threshold Time parameter: page A-13

The value you specify should be greater than the Version 1 query rate of all IGMP speakers on all networks directly connected to the router.

Configuring Logging

You can use Site Manager to specify the messages you want IGMP to log.

Site Manager: Debug parameter: page A-14

Configuring IGMP on an Interface

The following sections show you how to configure interface-specific IGMP features using Site Manager.

Enabling and Disabling IGMP

IGMP is automatically enabled when you add it to an IP interface. You can use Site Manager to disable and reenable IGMP on the interface.

Site Manager: Enable parameter: page A-15

Specifying a Query Rate

By default, IGMP sends out group membership queries on the interface every 120 seconds. You can use Site Manager to specify a query rate from 0 to 4096 seconds.

Site Manager: Interface Query Rate parameter: page A-16

Specifying 0 affects queries only. The router still forwards multicast datagrams on this circuit.

Note: If another IGMP router on this network has taken on the query role, this router will not send out queries unless it has not heard of any within the number of seconds specified by the Designated Router Timeout parameter.

Specifying a Membership Timeout Interval

By default, a local group membership is valid for 260 seconds without the receipt of a subsequent report for that group. You can use Site Manager to specify an interval from 50 to 8192 seconds.

Site Manager: Interface Membership Timeout parameter: page A-16

The suggested value is (2 * Query Rate) + 20.

Specifying a Designated Router Timeout Interval

By default, 140 seconds can elapse after the last host query message before the IGMP designated router is considered to be down. You can use Site Manager to specify a timeout interval from 10 to 8192 seconds.

Site Manager: Designated Router Timeout parameter: page A-16

The value you specify should be greater than the query rate of all IGMP routers on the network.

Specifying a Maximum Host Response Time

By default, a host must wait 100 tenths of a second before responding to a query. IGMP places this value in the code field of an IGMP query. You can use Site Manager to specify a value from one to 100 tenths of a second.

Site Manager: Max Host Response Time parameter: page A-17

Configuring a Static Host Entry

A network may include a member of a multicast group that is unable to register its network with the local IGMP router, for example, a host that is a member of a multicast group but that is not running IGMP.

In this situation, you can register the group member's network statically on the router.

A registration entry includes

- The circuit for the network containing the group member
- The group's multicast address and prefix

You can use Site Manager to supply this information.

Site Manager: Static Group CCT parameter: page A-14
Site Manager: Static Group Address parameter: page A-14
Site Manager: Static Group Prefix parameter: page A-15

Chapter 4
Customizing DVMRP

This chapter consists of the following sections describing the Distance Vector Multicast Routing Protocol (DVMRP):

- DVMRP Concepts and Terminology -- page 4-2
  - Neighbor Connections -- page 4-2
  - Source Route Advertisements -- page 4-4
  - How DVMRP Chooses a Route -- page 4-4
  - Routing Table and Forwarding Table -- page 4-5
  - Shortest-Path Trees -- page 4-6
- Configuring DVMRP on the Router -- page 4-7
  - Setting the Update Interval -- page 4-7
  - Configuring Tree Pruning -- page 4-8
  - Configuring DVMRP Timers -- page 4-9
  - Specifying a Probe Interval -- page 4-11
  - Specifying a Route Switch Interval -- page 4-11
  - Estimating the Number of Routes -- page 4-11
  - Logging Debugging Messages -- page 4-12
  - Specifying an MTU Size -- page 4-12
  - Specifying the Maximum Number of Routes -- page 4-12
- Configuring DVMRP on a Circuit -- page 4-13
  - Calculating a Route Metric and Comparing Route Costs -- page 4-13
  - Specifying a Threshold -- page 4-14
  - Configuring a Forwarding Table -- page 4-15
  - Disabling Advertisement of Local Networks -- page 4-16

- Configuring a Tunnel -- page 4-16

  Selecting the Encapsulation Mode -- page 4-16
  Specifying the Cost -- page 4-17
  Specifying a TTL -- page 4-17
  Configuring a Forwarding Table for the Tunnel -- page 4-17
  Supplying Addresses for the Tunnel -- page 4-18

DVMRP Concepts and Terminology

DVMRP is a dense-mode multicasting protocol. This protocol provides a mechanism for routers to propagate multicast datagrams in a manner that minimizes the number of excess copies sent to any particular network.

Neighbor Connections

In a DVMRP environment, *neighbors* are multicasting routers that are connected directly or through a tunnel:

- *Directly connected* neighbors are routers that have an interface to the same network.
- *Tunnel-connected* neighbors are multicast routers that communicate through a unicast network, exchanging DVMRP messages that are encapsulated in IP datagrams.

In Figure 4-1, for example, multicasting Router A has two neighbors, Router B and Router C. Router A and Router B are connected directly -- they both have interfaces to Net 6. Router A and Router C communicate through a tunnel that includes a unicast router.

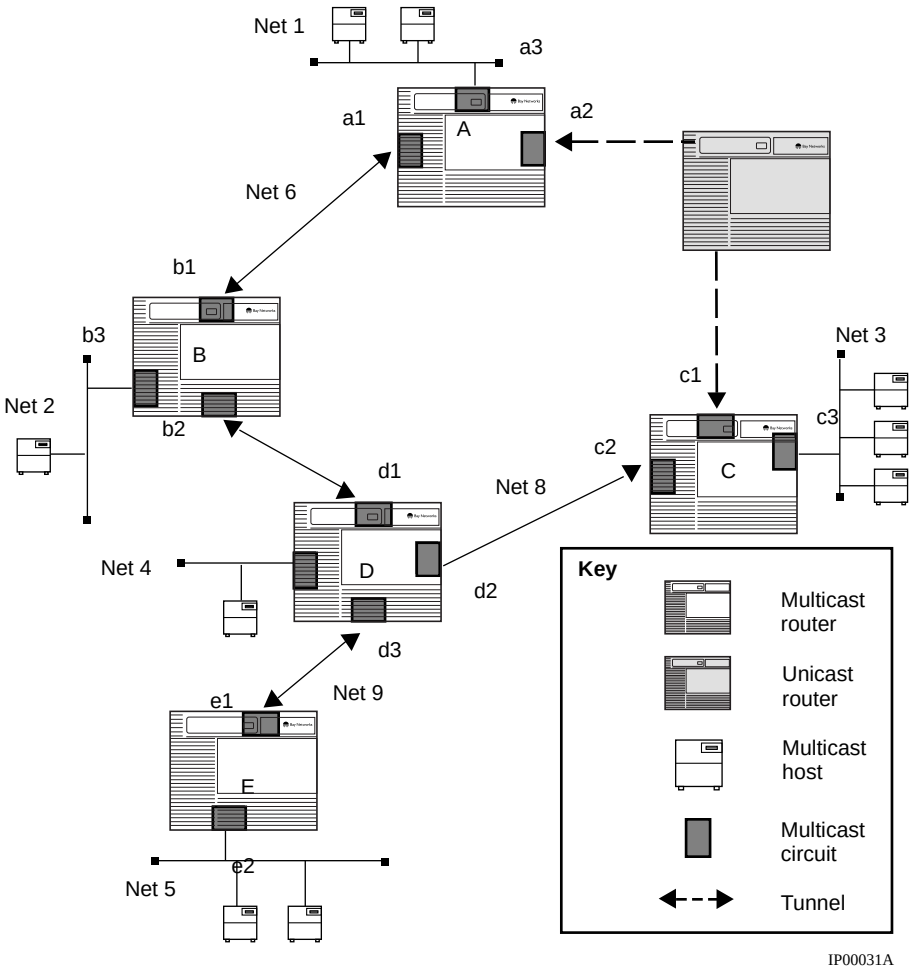

Figure 4-1. Multicast Routers

At startup, a DVMRP multicasting router

1. Initializes its routing table with information on all of its local networks
2. Learns the existence of its neighbors by sending a probe for all routes on each of its multicast interfaces (both physical circuits and tunnels)
3. Receives reports from its neighbors containing the routing information (including route costs)

In Figure 4-1, for example, Router D becomes active and issues routing probes on four multicasting interfaces. Router D receives reports from its multicasting neighbors, Routers B, C, and E.

Source Route Advertisements

A *source network* is any network containing hosts that have the capability to issue multicast datagrams. DVMRP advertises shortest-path routes to multicasting source networks. In this respect, DVMRP is the opposite of RIP, which advertises routes to destination networks.

Periodically, each multicasting router issues full or partial routing information on each DVMRP circuit, using DVMRP report messages. This routing information represents the sending router's cost to reach the specified source network. The cost is the sum of the hop metrics along the shortest path to the given source network.

Upon receiving a DVMRP report from another router, DVMRP reexamines its routing table to determine if the shortest path information needs updating. Specifically, DVMRP looks in the routing table for an entry describing a route to the same source network. If a route exists, DVMRP compares the cost of the two routes. DVMRP stores the route with the lower cost in its routing table.

A router will not send out route reports on an interface until it knows (by means of received probes or reports) that it has a neighboring multicast router on that interface. However, a router will continue to send probes periodically on an interface.

How DVMRP Chooses a Route

Each DVMRP interface is configured with a metric that indicates the cost of the hop. A router that receives multiple route reports for the same multicasting source network compares the cost specified in each (based on the metric field) and stores information from the report with the lowest cost in its routing table.

A route metric is the sum of all the interface (hop) metrics from a given route source to a given router. Currently, DVMRP restricts a route via multicast hosts (*mrouted*) to a total metric value of 31 or less.

In Figure 4-1, for example, Router D receives two reports for the network connected to multicasting Router A, one from Router B, and one from Router C. Using the metrics contained in the route reports, Router D determines that the cost of the tunneled route is greater than the cost of the route that uses direct physical connections. Router D discards the route received from Router C and stores the route received from Router B.

Router D then declares Router B to be the next-hop neighbor and Interface d1 to be the next-hop interface. Once a next-hop neighbor has been declared for a route, the route updates received from that neighbor for that route take precedence, until either the route times out or another router advertises a better metric for that route.

Routing Table and Forwarding Table

Table 4-1 summarizes the principal items in a routing table entry.

Table 4-1. Routing Table Entry Items

Item	Description
Source subnet address and mask	Address and mask of a subnetwork containing a host sourcing multicast datagrams
From-gateway	Previous-hop router leading back to the source subnet
TTL	Number of seconds before this entry is removed from the routing table

Note that the source subnet and the previous-hop router in the DVMRP routing table are the opposite of the destination subnet and next-hop router in a RIP routing table.

Using this information, the router can

1. Receive a multicast datagram and determine if the datagram has arrived on the interface that is on the shortest path to the source network.
2. Drop the datagram if it has not arrived on the shortest-path interface.
3. Flood the multicast datagram to all active DVMRP neighbors.

Once DVMRP has received a multicast datagram on an interface and flooded the datagram to its neighbor, DVMRP makes an entry for the datagram in the forwarding table for the interface.

Table 4-2 summarizes the principal items in a forwarding table entry.

Table 4-2. Forwarding Table Entry Items

Item	Description
Source subnet	Subnet containing a host that is the source of multicast datagrams addressed to the specified groups
Multicast group	Class D destination address identifying the group to which the datagram is being sent
Inbound interface	Interface on which the multicast datagram arrived
Outbound interfaces	Interfaces from which the multicast datagram is forwarded

Shortest-Path Trees

Route information used by DVMRP is independent of any other routing information used by the router -- for example, routes provided by RIP. The purpose of this routing information is to create a shortest-path tree entry in the routing table for the propagation of multicast datagrams. The shortest-path tree entry indicates the interface that provides the shortest path to the network that is the source of the multicast datagram.

In Figure 4-1, for example, the routing table on Router D includes an entry describing the shortest-path route to the network connected to Router A. The entry indicates that Interface d1 provides the shortest path to that source network.

A shortest-path tree also indicates those interfaces that are on the shortest path to that source network from a neighboring router. For example, Router E considers the network connecting it to Router D to be on the shortest path to the source network connected to router A. Router D has an interface (d3), that is part of the shortest path from Router E from the network connected to Router A.

If neighboring routers have the same metric to a given source network, the router with the lower IP address will be responsible for propagating multicast traffic originating from that source network onto the network or tunnel that is common to these neighboring routers.

A network that is not on the shortest path to a source network from a multicast router is considered to be a leaf. In Figure 4-1, the network connected to Router E (Net 5) is a *leaf network*.

Configuring DVMRP on the Router

When you select DVMRP, support for the protocol is automatically enabled on the router.

You can use Site Manager to disable and reenable DVMRP on the router.

Site Manager: Enable parameter: page A-2

Setting the Update Interval

Periodically, each multicasting router issues full or partial routing information on each DVMRP circuit, using DVMRP report messages. This routing information represents the sending router's cost to reach the specified network (the cost is the sum of the hop metrics along the shortest path to the given source network).

You can use Site Manager to

- Specify how often routing messages containing complete routing tables are sent.
- Specify the minimum amount of time between triggered updates. *Triggered updates* are sent in the period between full updates. Issuing a full update restarts the triggered update timer. Therefore, the triggered update interval you specify must be shorter than the full update interval you have specified.

Site Manager: Full Update Interval parameter: page A-2
Site Manager: Triggered Update Interval parameter: page A-2

Configuring Tree Pruning

If a host drops out of a multicast group, multicast routers may continue to forward group messages to that host. DVMRP routers use a technique called *pruning* to avoid the waste of network resources caused by the transmission of group messages to hosts that are no longer members of the group.

The following conditions cause DVMRP to prune the shortest-path tree for a given group:

- The router determines that the attached network on which the host is located (or any other locally attached network) has no active group member.
- The router determines that all neighbors on all attached networks other than the next-hop network to the source have pruned off the source and group.
- The router determines that it is not located on the shortest network path to any remote network that includes a member of the group.
- The router sends a DVMRP PRUNE message to its DVMRP neighbor. The neighbor removes the router from its forwarding table.

  If the host later rejoins the group, the router sends the neighbor a DVMRP GRAFT message. The router restores the host to its forwarding table.

Tree pruning is enabled on the router by default. You can use Site Manager to disable and reenable tree pruning on the router.

Site Manager: Pruning Enable parameter: page A-6

Configuring DVMRP Timers

When a router adds or updates a route, it uses configurable aging timers to control the useful life of the route.

Setting the Route Expiration Timer

The route expiration timer determines how long DVMRP waits for an update message indicating that a route is reachable. Upon expiration of this timer, this route is advertised as unreachable until it is refreshed or until it is deleted.

By default, DVMRP sets the route expiration time at 200 seconds.You can use Site Manager to set the route expiration time from 20 to 4000 seconds.

Site Manager: Route Expiration Timeout parameter: page A-3

Setting the Garbage Timer

The garbage timer determines how long DVMRP advertises a route as unreachable before it removes the route from the routing table. The difference between the garbage timer and the route expiration timeout value represents the amount of time that the route will be advertised as unreachable without subsequent refreshment.

By default, DVMRP sets the garbage timer to 340 seconds. You can use Site Manager to set the value from 40 to 8000 seconds.

Site Manager: Garbage Timeout parameter: page A-4

Enter a value that is greater than the value you specified for the route expiration timer to allow enough time for the route to be advertised as unreachable.

Setting the Neighbor Report Timer

The neighbor report timer specifies how long the router waits to receive a report from a neighbor before considering the connection inactive.

By default, DVMRP waits 140 seconds. You can use Site Manager to specify a value from 40 to 8000 seconds.

Site Manager: Neighbor Timeout parameter: page A-3

Setting the Leaf Timer

The leaf timer determines whether a network or tunnel local to a given interface is considered to be part of the shortest path to a given source network by any DVMRP neighbor.

If during this time the local interface has not received a route report for a given source network, this network or tunnel and its local interface are considered not to lie in the shortest path for any neighbor. In other words, the local network is not part of the shortest path to that specific source network.

By default, DVMRP sets the leaf timer at 200 seconds. You can use Site Manager to specify a value from 25 to 4000 seconds.

Site Manager: Leaf Timeout parameter: page A-3

Specifying a Probe Interval

The probe interval determines how often DVMRP sends a probe on interfaces from which no neighbors have been heard.

By default, DVMRP sends a probe every 10 seconds. You can use Site Manager to specify a value from 5 to 30 seconds.

Site Manager: Neighbor Timeout parameter: page A-3

If your neighbor is running DVMRP *mrouted*, ensure that your probe interval value matches the value used by the neighbor.

Specifying a Route Switch Interval

The route switch interval specifies how long to wait, without receiving a subsequent route update from the original neighbor, before switching to a different neighbor advertising equal cost for this route.

By default, DVMRP waits 140 seconds. You can use Site Manager to specify a value from 20 to 2000 seconds.

Site Manager: Route Switch Timeout parameter: page A-5

If your neighbor is running DVMRP *mrouted*, the recommended value is 140 seconds.

Estimating the Number of Routes

By default, DVMRP preallocates a routing table for 25 entries. You can use Site Manager to specify the number of entries (10 or greater).

Site Manager: Estimated Routes parameter: page A-4

Enter a value that the router can use for preallocating routing tables. For an MBone (multicasting backbone) deployment, a value of 3000 or higher is recommended.

Note that routes are kept on a per-source-network basis, independent of multicast groups. The number of routes must include a route for every network that is local to a circuit configured for multicasting. This allows the router to utilize memory efficiently. Exceeding this size during router operation will not cause an error but may cause the router to consume more memory than is required.

Logging Debugging Messages

By default, DVMRP does not log debugging messages. You can use Site Manager to enable the logging of debugging messages and to specify the level of debug messages.

Site Manager: Debug Level parameter: page A-5

Specifying an MTU Size

By default, DVMRP uses a maximum transmission unit (MTU) size of 1514. The default maximum size is the CSMACD_MTU size. The minimum size is the X25_DDN_MTU size.

You can use Site Manager to specify an MTU size in the range of 910 to 1514 bytes.

Site Manager: Fragmented MTU Threshold parameter: page A-6

Specifying the Maximum Number of Routes

By default, DVMRP stores all learned routes in the routing table. You can use Site Manager to specify the number of routes that DVMRP can learn per slot. This parameter limits the number of routes that can be stored in the routing table.

Site Manager: Max Routes parameter: page A-6

If you specify a maximum number of routes, you must include a route for every local network that has a circuit configured for multicasting.

Configuring DVMRP on a Circuit

The following sections describe DVMRP circuit-specific features.

Enabling and Disabling DVMRP

By default, DVMRP is enabled on a circuit. You can use Site Manager to disable and reenable it.

Site Manager: Enable parameter: page A-7

Disabling Multicast Support

By default, DVMRP

- Propagates multicast routing information on the circuit
- Incorporates information about the source network associated with this circuit in routing updates
- Forwards multicast datagrams on this circuit in *native mode* -- that is, as multicast datagrams

You can configure a tunnel on a circuit enabled for multicasting.

Using Site Manager, you can disable multicast support on the circuit if you want the circuit to exist only to support unicast tunnels.

Site Manager: Route Enable parameter: page A-7

Calculating a Route Metric and Comparing Route Costs

By default, a circuit has a cost of 1. You can use Site Manager to assign a cost in the range of 1 to 31.

Site Manager: Metric parameter: page A-8

We recommend the following values:

Hop	Metric
LAN, or tunnel across a single LAN	1
Multihop tunnel	2 or 3
Serial link, or tunnel across a serial link	1
Backup tunnel	Primary tunnel metric + 1

Specifying a Threshold

Threshold values control the scope of datagram delivery. The threshold is the minimum IP time-to-live (TTL) required for a multicast datagram to be forwarded out a given interface. DVMRP compares the TTL value of each multicast datagram to be forwarded with the threshold configured for that interface. If the IP TTL is less than the threshold value you specify, the datagram is dropped by the router.

For *mrouted* compatibility, multicast datagrams originated by the router have a TTL of 1. These datagrams are not compared against the TTL. Unicast datagrams originated by the router (for example, for route reports issued via a tunnel) have a TTL of 255. A datagram that is to be forwarded through a tunnel is first compared against the threshold and, if accepted, is then encapsulated in an IP datagram with a TTL of 64.

By default, DVMRP uses a TTL value of 1. You can use Site Manager to specify a TTL value from 1 to 254.

Site Manager: Threshold parameter: page A-8

Table 4-3 lists the originating TTL values recommended for certain types of multicast applications and the threshold values recommended for routers to permit the forwarding of packets from these applications. These values are recommended for topologies that will connect to the MBone.

Table 4-3. Recommended TTL and Threshold Values

Multicast Application	TTL	Threshold
IETF channel 1 low-rate GSM audio	255	224
IETF channel 2 low-rate GSM audio	223	192
IETF channel 1 PCM audio	191	160
IETF channel 2 PCM audio	159	128
IETF channel 1 video	127	96
IETF channel 2 video	95	64
Local event audio	63	32
Local event video	31	1

Configuring a Forwarding Table

To keep to a minimum the amount of time that it spends looking up routes, DVMRP creates and maintains a cache of frequently used routes -- called a *forwarding table* -- for each IP interface.

By default, DVMRP preallocates a forwarding table of 32 entries for each circuit. You can use Site Manager to specify the maximum number of entries (32 to 512) allowed in the forwarding table associated with this circuit.

Site Manager: Forward Cache Size parameter: page A-11

When configuring a cache size, you must also keep in mind the TTL value for entries. If you specify a large cache size, you can specify a larger TTL value. A smaller cache requires a smaller TTL for cache entries.

By default, DVMRP uses a TTL of 300 seconds for entries in the forwarding table. You can use Site Manager to specify a TTL in the range of 300 to 86400 seconds.

Site Manager: Forward Cache TTL parameter: page A-9

If your neighbor is running *mrouted*, the recommended TTL value is 300 seconds.

Disabling Advertisement of Local Networks

By default, DVMRP advertises its own local networks over this circuit. Using Site Manager, you can configure DVMRP so that it does not advertise local networks over the circuit.

Site Manager: Advertise Self parameter: page A-9

Configuring a Tunnel

The following sections explain how to use Site Manager to configure a DVMRP tunnel.

Enabling and Disabling the Tunnel

When you configure a tunnel on a circuit, the tunnel is enabled by default. You can use Site Manager to disable and reenable the tunnel.

Site Manager: Enable parameter: page A-10

Selecting the Encapsulation Mode

By default, DVMRP encapsulates a tunneled multicast datagram in an IP unicast datagram. Using Site Manager, you can configure DVMRP to loosely encapsulate multicast datagrams using the LSSR option.

Site Manager: Encapsulation Mode parameter: page A-10

See RFC 1075 for information about the LSSR option, which is provided for backward compatibility.

Specifying the Cost

By default, DVMRP assigns a metric of 1 to a tunnel. You can use Site Manager to specify a cost value from 1 to 31.

Site Manager: Metric parameter: page A-10

Specifying a TTL

By default, DVMRP assigns a TTL value of 1 to a tunnel. This value is the minimum IP TTL required for a multicast datagram to be forwarded out this tunnel. You can use Site Manager to assign a value from 1 to 254.

Site Manager: Threshold parameter: page A-11

Use this value to control the scope of the datagrams. If the IP TTL is less than the threshold value you specify, the router drops the datagram.

Configuring a Forwarding Table for the Tunnel

By default, DVMRP preallocates a forwarding table for 32 entries. You can use Site Manager to specify the maximum number of entries (from 32 to 512) allowed in the forwarding table associated with this tunnel interface.

Site Manager: Forward Cache Size parameter: page A-11

When configuring a cache size, you must also keep in mind the TTL value for entries. If you specify a large cache size, you can specify a larger TTL value. A smaller cache requires a smaller TTL for cache entries.

By default, DVMRP assigns a TTL value of 300 seconds to an entry in a tunnel forwarding table. You can use Site Manager to assign a value in the range of 300 to 86400 seconds.

Site Manager: Forward Cache TTL parameter: page A-11

Supplying Addresses for the Tunnel

To identify a unicast tunnel, you must supply the unicast IP address of both ends of the tunnel: the local interface and the remote interface. You can use Site Manager to supply these addresses.

Site Manager: Remote IP address parameter: page A-12

Chapter 5
Customizing ST2 Services

This chapter consists of the following sections describing services provided by the Internet Stream Protocol (ST2):

- ST2 Concepts and Terminology -- page 5-2
  - ST2 and IP -- page 5-2
  - ST2 Agents -- page 5-2
  - Stream Control Messages -- page 5-4
  - Neighbors and Tunnels -- page 5-4
  - ST2 Features -- page 5-6
- The Role of an ST2 Intermediate Agent -- page 5-7
  - How the Agent Sets Up a Stream Segment -- page 5-7
  - How the Agent Adds a Target to a Stream -- page 5-10
  - How the Agent Forwards ST2 Data Downstream -- page 5-12
  - How the Agent Shuts Down a Stream -- page 5-12
- Configuring ST2 on the Router -- page 5-12
  - Enabling and Disabling ST2 -- page 5-12
  - Configuring the Tunnel Capability -- page 5-13
- Configuring an ST2 Interface -- page 5-13
  - Enabling and Disabling ST2 -- page 5-13
  - Specifying an IP Address -- page 5-13
  - Setting Interface Timers and Counters -- page 5-14
- Configuring the Neighbors Forwarding Table -- page 5-15

ST2 Concepts and Terminology

The Internet Stream Protocol (ST2) enables a network application to reserve resources on internet routers for an ST2 stream -- a transmission path from a data origin to one or more data targets. The capability to reserve Internet resources makes ST2 well suited for video conferencing, real-time simulation, and other multimedia applications.

An ST2 stream is a point-to-point or point-to-multipoint connection. Figure 5-1 shows an ST2 stream established between a single video stream unit -- the origin of the transmissions -- and six receiving target video systems. The stream is simplex -- data flows in one direction only, downstream from the origin to the targets.

ST2 and IP

Underlying and supporting an ST2 stream is an internet topology that includes multiple IP routers capable of providing and guaranteeing the resources required for the data transmission. For example, the topology underlying the stream in Figure 5-1 includes seven routers.

An ST2 stream creates a semblance of an end-to-end connection establishment typical of a virtual circuit protocol. However, messages are never exchanged directly between origin and targets. Each router discovers the next-hop IP routers and is concerned only with the part of the stream between itself and these routers.

ST2 Agents

Each IP router supporting the stream is configured with the hardware and software required for ST2 data transmissions; in addition, each router is running ST2 agent software. Such routers are considered to be *ST2 capable*.

An ST2 agent that receives control messages and stream data directly from an origin application or delivers control messages and stream data to a target application is considered to be a host agent. ST2 agents that forward control messages and data to the next agent downstream are considered to be intermediate agents. A Bay Networks router can be configured as an intermediate ST2 agent. The ST2 environment in Figure 5-1 includes three Bay Networks routers (BayNet/ST2 1, BayNet/ST2 2, and BayNet/ST2 3).

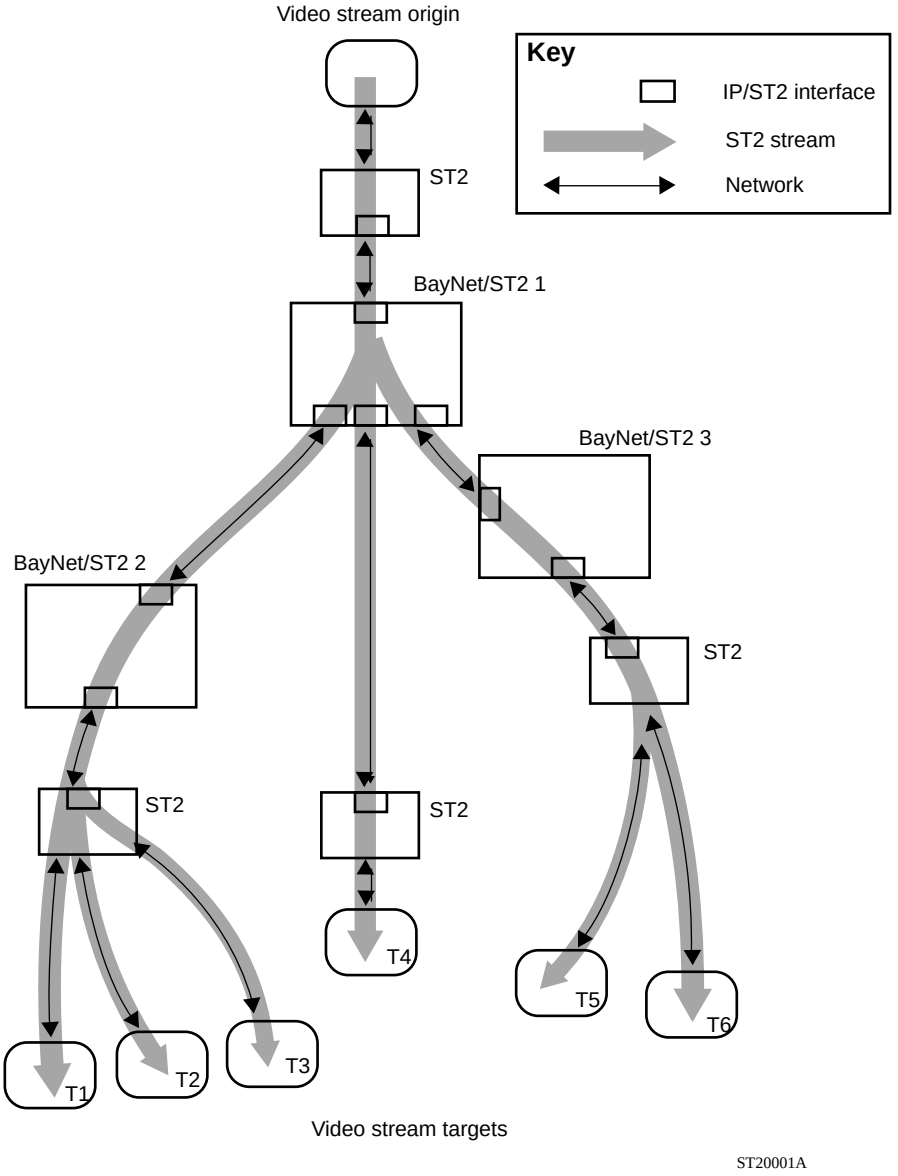

Figure 5-1. ST2 Point-to-Multipoint Stream

Stream Control Messages

ST2 agents communicate with each other by exchanging messages defined by the Stream Control Message Protocol (SCMP).

For example, an origin that wants to establish a stream sends an SCMP connect message to the next-hop IP router downstream. The connection request includes

- A list of one or more targets.
- A hop identifier (HID). An HID is suggested by the upstream agent. The downstream agent may accept the HID or propose an alternative HID.
- A flowspec listing the network resources required for the stream.

To accept a connection request from an upstream agent, the agent returns an SCMP ACCEPT message.

In "ST2 Features" on page 5-6, Table 5-1 lists all the SCMP messages currently supported by the Bay Networks implementation of ST2.

Neighbors and Tunnels

An ST2 agent exchanges SCMP messages with next-hop agents. In an ST2 environment, next-hop agents are considered to be neighbors.

Neighbors can be connected in two ways -- directly or through an ST2 tunnel. In Figure 5-2 the ST2 agent on Router A has two neighbors, the agent on Router B and the agent on Router D. Router A and Router B are connected directly -- they both have an interface to Network 1. Router A and Router D are connected through a tunnel that includes Network 2 and Network 3, and a router that does not have ST2 capabilities, Router C.

Tunnels are configured by the network administrator to establish ST2 streams in networks where not all IP routers are ST2 capable. For transmission through a tunnel, SCMP messages and ST2 data are encapsulated in IP datagrams and forwarded through a non-ST2 router, and decapsulated at the destination.

A non-ST2 router can provide a tunnel for both stream data and control messages; however, a router that lacks ST2 capability cannot guarantee the resources listed in the flowspec.

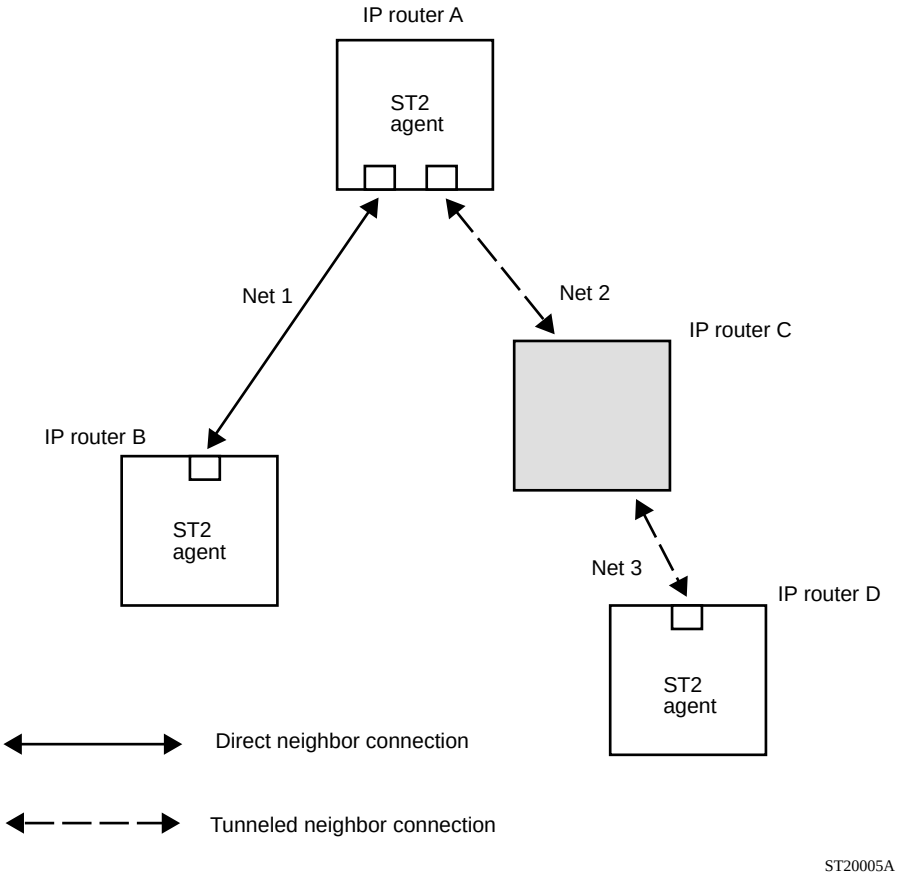

Figure 5-2. ST2 Neighbors

Resource Manager

An SCMP CONNECT request includes a flowspec that lists the communications resources required by the proposed stream.

On a Bay Networks router, an ST2 agent that receives a connect request from an agent upstream passes the flowspec to the local Resource Manager.

The Resource Manager allocates and guarantees the resources required by the stream.

For information on the Resource Manager, see Chapter 6.

ST2 Features

Table 5-1 lists ST2 features and indicates the ones called out in RFC 1190, "Experimental Internet Stream Protocol, Version 2," and the ones supported by the current version of Bay Networks router software.

Table 5-1. ST2 Features

Feature	RFC 1190	Bay Networks
Multiline circuits	n/a	yes
Peak bandwidth reservation	n/a	yes
Bandwidth policing	n/a	yes
Autorouting using IP route tables	n/a	yes
IP encapsulation of ST2	yes	yes
Adding targets during connection	yes	yes
HID negotiation	yes	yes
SCMP(ACCEPT)	yes	yes
SCMP(ACK)	yes	yes
SCMP(CHANGE REQUEST)	yes	no
SCMP(CHANGE)	yes	no
SCMP(CONNECT)	yes	yes
SCMP(DISCONNECT)	yes	yes
SCMP(ERROR IN REQUEST)	yes	yes
SCMP(ERROR IN RESPONSE)	yes	yes
SCMP(HELLO)	yes	yes
SCMP(HID-CHANGE)	yes	yes
SCMP(HID-APPROVE)	yes	yes
SCMP(HID-REJECT)	yes	yes
SCMP(HID-CHANGE-REQUEST)	yes	no
SCMP(NOTIFY)	yes	no
SCMP(REFUSE)	yes	yes
SCMP(STATUS)	yes	no
SCMP(STATUS-RESPONSE)	yes	no
SCMP (OPCODE 18:userdata)	no	yes

The Role of an ST2 Intermediate Agent

This section examines the role played by an intermediate ST2 agent running on a Bay Networks router in an ST2 environment.

How the Agent Sets Up a Stream Segment

As part of ST2 stream setup, a Bay Networks router configured as an intermediate agent

1. Receives an SCMP connect request from an upstream ST2 neighbor
2. Establishes a connection with the upstream neighbor
3. Determines the appropriate downstream neighbor
4. Reserves resources on the downstream interface
5. Sends an SCMP connection request to the downstream neighbor
6. Establishes a connection with the downstream neighbor

Stream setup creates a semblance of an end-to-end connection establishment typical of a virtual circuit protocol. However, control messages are never exchanged directly between origin and targets.

Receiving a Connect Request from Upstream

An intermediate ST agent receives connect requests on ST2 interfaces from upstream agents. A connect request can specify a single target (the typical case) or multiple targets. In Figure 5-3, for example, BayNet/ST2 1, an intermediate agent, receives a connect request from ST2 1. The connect request specifies a single target for the stream, T6. The request also includes a flowspec listing the network resources required for the transmission.

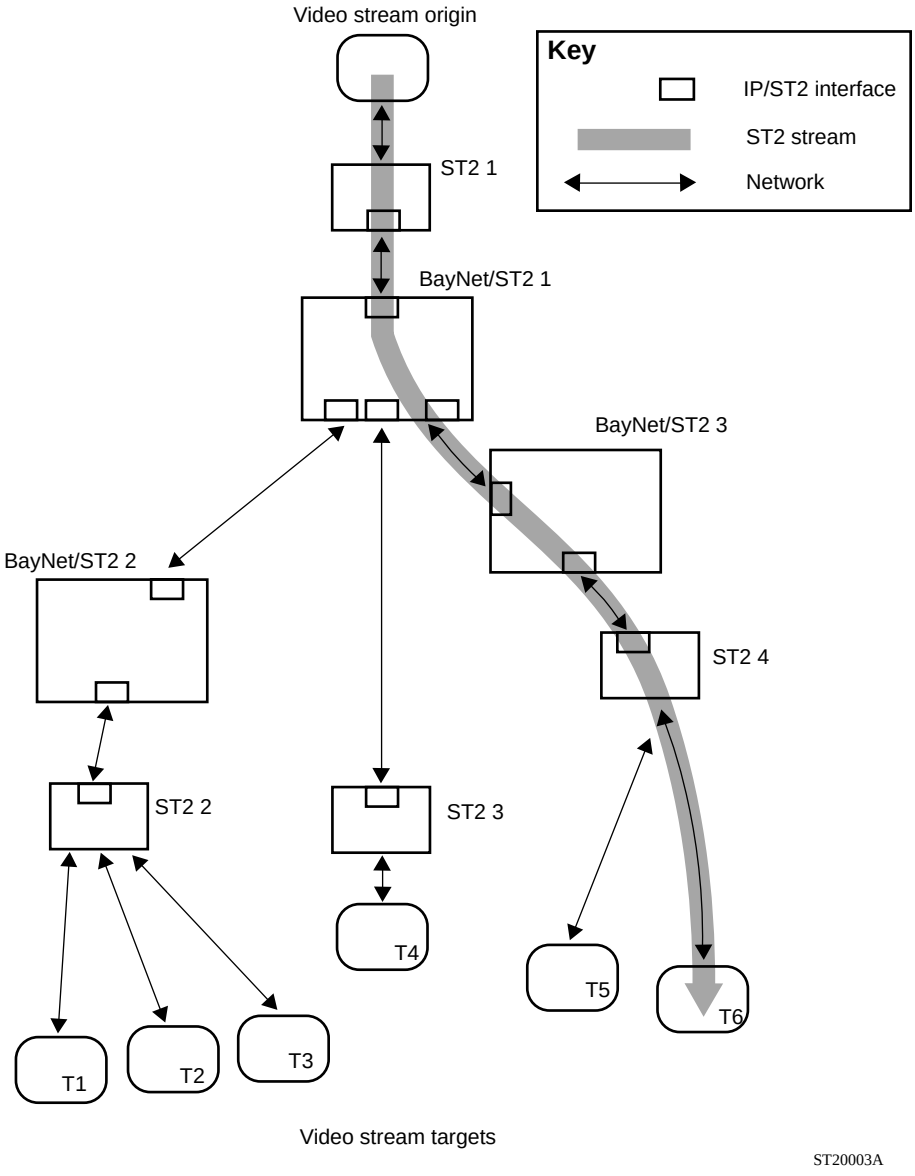

Figure 5-3. Setting Up a Point-to-Point Stream

The ST2 agent on BayNet/ST2 1, using the information in the connection request:

1. Negotiates a hop identifier (HID) with the previous hop, ST2 1
2. Reserves the local and network resources required to support the stream
3. Passes the flowspec to the Bay Networks resource manager

Determining the Next Hop Downstream

An ST2 agent on a Bay Networks router uses two methods to determine the next downstream hop in the stream:

- IP-inherited routing (the primary method), using the IP routing table
- ST2 exploratory routing (the backup method), using the ST2 neighbor table

Using the IP Routing Table (IP-Inherited Routing)

In IP-inherited routing, the ST2 agent obtains the address of the next-hop router from the IP routing table. This table consists of entries describing routes that have been learned by the routing protocols configured on the router (OSPF and BGP, for example). The routing table also contains entries for *static routes* -- that is, routes that have been inserted by the network administrator.

Each entry in the IP routing table includes a target IP network, a next-hop IP address, an interface address, and other information. There is no information in a routing table entry, however, to distinguish an ST2 route (that is, a hop with an ST2-capable router on the other end). For this reason, it is possible for ST2 to select a route that it cannot use.

If ST2 selects a route that is not ST2 capable (and does not provide a tunnel to an ST2 agent), ST2 does not use the route and returns an SCMP REFUSE message upstream with the reason code No Route to Destination.

If the required resources are not available via a path stored in the IP routing table, ST2 uses exploratory routing. See “Using the ST2 Neighbor Table (Exploratory Routing)” on page 5-10.

Using the ST2 Neighbor Table (Exploratory Routing)

In exploratory routing, the ST2 agent obtains information about its ST2-capable neighbors from its ST2 neighbors table. This table, which is configured by the network administrator, consists of entries that describe the characteristics of a next-hop neighbor and provide the next-hop address.

The table notes those neighbors that can perform exploratory routing. When resources are not available via a route stored in the IP routing table, the ST2 agent selects a neighbor that is capable of exploratory routing.

Establishing a Connection with a Downstream Neighbor

Once the SCMP session has been established, the downstream intermediate agent becomes the upstream agent for the next hop and issues a connect message. The message contains an HID value and the flowspec for the stream.

How the Agent Adds a Target to a Stream

Once a stream has been established from the origin to a target, the origin can issue additional connect requests to add targets to the stream. Each connect request identifies the stream and specifies the target to add. In Figure 5-4, for example, target T4 has been added to the stream established between the video origin and T6.

To create a new branch in the stream (if one is required), the intermediate ST2 agent follows the steps described in “Determining the Next Hop Downstream” on page 5-9 and in the previous section, “Establishing a Connection with a Downstream Neighbor.”

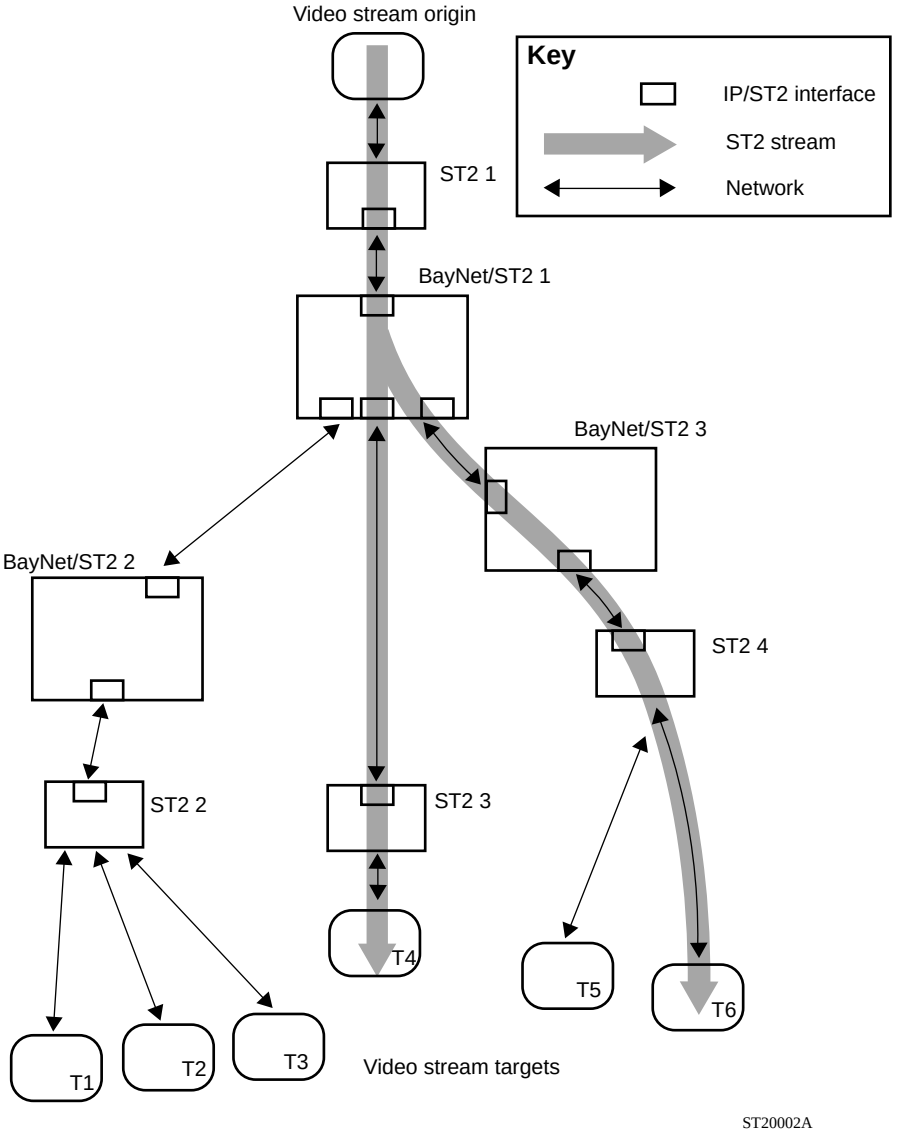

Figure 5-4. Adding a Target to a Stream

How the Agent Forwards ST2 Data Downstream

An ST agent receives data packets encapsulated by an ST header. A data packet received by an ST agent contains the HID assigned to the stream for the branch from the previous hop to itself. The agent uses the HID to quickly obtain the necessary forwarding information for the next hop.

The forwarding information identifies the next-hop agent and includes the HID and address of the next hop.

How the Agent Shuts Down a Stream

Two SCMP messages -- Disconnect and Refuse -- allow ST2 agents to shut down a stream in an orderly manner:

- An intermediate agent receives SCMP Disconnect messages on its upstream ST2 interfaces. Disconnect messages can be generated by the origin or, in the case of network failure, by a next-hop agent upstream.
- An intermediate agent receives SCMP Refuse messages on its downstream ST2 interfaces. Refuse messages can be generated by an ST2 target or by a next-hop agent downstream.

The ST2 agent acknowledges the request to shut down the stream and performs the appropriate action. In the case of a Disconnect message, the agent sends a Disconnect message to the next-hop agent or agents downstream. In the case of a Refuse message, the agent sends a Refuse message to the next hop upstream.

Configuring ST2 on the Router

The following sections describe global ST2 features that you can configure on the router.

Enabling and Disabling ST2

By default, the router starts ST2 on the slot when you configure an ST2 interface on a circuit.

You can use Site Manager to disable and reenable ST2 on the slot.

Site Manager: Enable parameter: page A-19

Configuring the Tunnel Capability

By default, ST2 does not have tunneling capability. If your network requires the use of tunnels to establish a neighbor-to-neighbor connection, you can use Site Manager to configure the feature.

Site Manager: Tunnelling Capability parameter: page A-19

If you enable the tunnel capability on the router, you can use Site Manager to disable and reenable the feature.

Site Manager: Tunneling Enable parameter: page A-20

Configuring an ST2 Interface

The following sections describe ST2 features that you can configure on an ST2 interface.

Enabling and Disabling ST2

By default, the router enables ST2 when you add an ST2 interface to the circuit.

You can use Site Manager to disable and reenable ST2 on the interface.

Site Manager: Enable parameter: page A-20

Specifying an IP Address

You can use Site Manager to specify the IP address of this ST2 interface.

Site Manager: IP Address parameter: page A-20

Setting Interface Timers and Counters

Table 5-2 lists the ST2 timers you can set using Site Manager.

Table 5-2. ST2 Timers

Timer	Description	Parameter Name and Link to Instructions
Accept message retries timer	The time in seconds between ST2 accept message retries on this interface	Site Manager: Accept Time Out parameter: page A-21
Accept message retries counter	The maximum retry count for accept messages on this interface	Site Manager: Accept Retry parameter: page A-21
Connect message retries timer	The time in seconds between ST2 connect message retries on this interface	Site Manager: Connect Time Out parameter: page A-21
Connect message retries counter	The maximum retry count for connect messages on this interface	Site Manager: Connect Retry parameter: page A-21
Disconnect message retries timer	The time in seconds between ST2 disconnect message retries on this interface	Site Manager: Disconnect Time Out parameter: page A-22
Disconnect message retries counter	The maximum retry count for HID change messages on this interface	Site Manager: Disconnect Retry parameter: page A-22
HID change message retries timer	The time in seconds between ST2 HID change message retries on this interface	Site Manager: HID Change Time Out parameter: page A-22
HID change message retries counter	The maximum retry count for HID change messages on this interface	Site Manager: HID Change Retry parameter: page A-23
Refuse message retries timer	The time in seconds between ST2 refuse message retries on this interface	Site Manager: Refuse Time Out parameter: page A-23
Refuse message retries counter	The maximum retry count for refuse messages on this interface	Site Manager: Refuse Retry parameter: page A-23
Hello message retries timer	The time in seconds between ST2 hello message retries on this interface	Site Manager: Hello Time Out parameter: page A-24
Hello message retries counter	The maximum retry count for hello messages on this interface	Site Manager: Hello Retry parameter: page A-24

Configuring the Neighbors Forwarding Table

You can use Site Manager to store the following information about an ST2 neighbor in the neighbors forwarding table:

- Whether the record for this neighbor is active.
- Whether the neighbor is capable of route exploration.
- Whether the router should send Hello messages to the neighbor. The hello Protocol parameter also specifies the type of hello procedure. Select Enable to use the normal Bay Networks hello procedure. Select Hello When Stream Active to use the hello procedure only when a stream is running to a neighbor.
- The type of connection to this neighbor.
- A priority value for the neighbor. If you enter multiple ST2 route exploration neighbors in the forwarding table, use the Neighbor Priority Level parameter to rank them. First choice is the neighbor with the lowest value.
- The IP address of the next-hop neighbor -- router or host.

Site Manager: Enable parameter: page A-24
Site Manager: Route Exploration Capability parameter: page A-25
Site Manager: Hello Protocol parameter: page A-25
Site Manager: Neighbor Type parameter: page A-25
Site Manager: Neighbor Priority Level parameter: page A-26
Site Manager: Next Hop IP Address parameter: page A-26

Chapter 6
Reserving Line Resources

The first part of this chapter provides an overview of the Resource Manager, a service for line resource reservation on Bay Networks routers.

Later sections explain

- Starting the Resource Manager -- page 6-3
- Configuring the Resource Manager -- page 6-6

  Setting the Estimated Bandwidth -- page 6-7
  Setting the Reservable Bandwidth -- page 6-7
  Specifying the Traffic Queuing Algorithm -- page 6-7
  Specifying the Policing Algorithm -- page 6-8
  Setting the Bandwidth Interval -- page 6-8
  Setting the Inflate Reservations Percentage -- page 6-9
  Specifying the Unreserved Policing Algorithm -- page 6-9
  Specifying the Unreserved Queue Length -- page 6-10
  Specifying the Multiline Select Algorithm -- page 6-10
  Setting the Multiline Threshold Bandwidth -- page 6-10
  Setting the Reservation Latency -- page 6-11

- Disabling Line Resource Management -- page 6-12

  Removing a Line's Reservations -- page 6-12
  Deleting Resource Manager Services -- page 6-12

About Line Resource Reservation

Emerging realtime multicast applications for digitized voice and video (such as multimedia conferencing and virtual reality) require a level of consistent network service that routers cannot meet using simple first-in-first-out (FIFO) queuing mechanisms. The existing best-effort delivery service of IP networks, where variable queuing delays and data loss due to congestion are acceptable, is not sufficient.

Resource reservation protocols such as Stream Protocol 2 (ST2) address the requirements of delay-sensitive applications by distributing information among routers to achieve a guaranteed quality of service (QoS) for specific packet streams (flows).

By reserving bandwidth for QoS requests, a system of line resource reservation can meet the demands of realtime applications and maintain bandwidth for other traffic.

Resource Manager

The Bay Networks Resource Manager lets you define a certain percentage of a line's bandwidth as *reservable*. Applications that require a guaranteed QoS can negotiate for the reservable bandwidth. When the router honors a reservation request, the Resource Manager allocates bandwidth from the reservable bandwidth, reducing the bandwidth available for other requests.

Supported Media

You can enable the Resource Manager on 10-Mb/s Ethernet, MCT1, HSSI, and synchronous interfaces that are configured with the ST2 protocol. The Resource Manager supports the following synchronous interface encapsulation methods:

- Point-to-Point Protocol (PPP)
- Bay Networks Standard
- Frame Relay
- ATM DXI

Note: You cannot use line resource management on a line you configured for PPP multilink.

How the Resource Manager Works with ST2

The following summarizes the exchange between the ST2 agent and the Resource Manager :

1. The router receives an ST2 connect request.

   The ST2 connect request includes a flow specification (*flowspec*) that indicates the resources needed to meet the QoS.

2. ST2 passes the flowspec to the Resource Manager.
3. The Resource Manager compares the requested resources with available reservable bandwidth.

   Resource Manager determines reservable bandwidth from configured values described later in this chapter. It also accounts for any active reserved flows.

4. The Resource Manager either reserves the necessary services or refuses service.

Starting the Resource Manager

Note: Before you can enable the Resource Manager, you must first configure IP and the ST2 agent on a circuit.

To enable the Resource Manager for reserving and allocating bandwidth:

1. **Start at the Configuration Manager window.**
2. **Click on the circuit connector.**

   Select any XCVR (10-Mb/s or 100-Mb/s Ethernet), HSSI, MCT1, or COM connector for a line that is configured for ST2.

3. **Unless you selected an MCT1 connector, go to Step 6.**

   The MCT1 Logical Lines window appears (Figure 6-1).

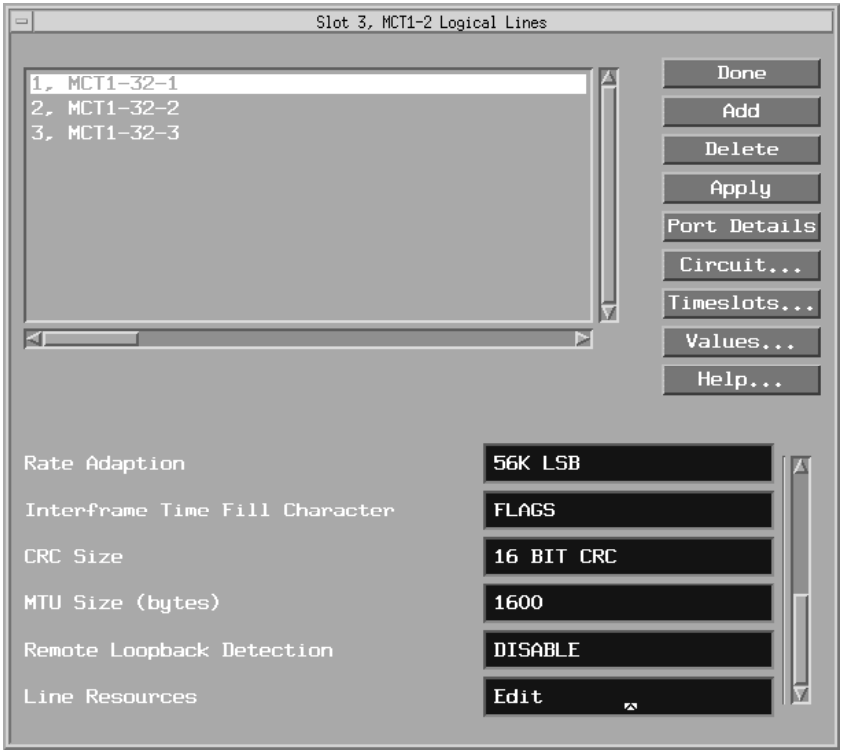

Figure 6-1. MCT1 Logical Lines Window

4. **Select the Line Resources box.**
5. **Click on Values.**
6. **Click on Edit Line Resources in the Edit Connector window (Figure 6-2).**

Figure 6-2. Edit Connector Window

The following Site Manager prompt appears (Figure 6-3):

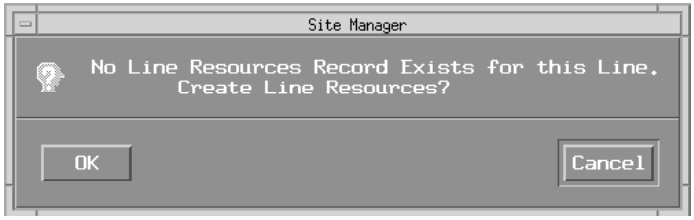

Figure 6-3. Creating the Line Resources Record

7. **Click on OK.**

The Edit Line Resources window appears (Figure 6-4).

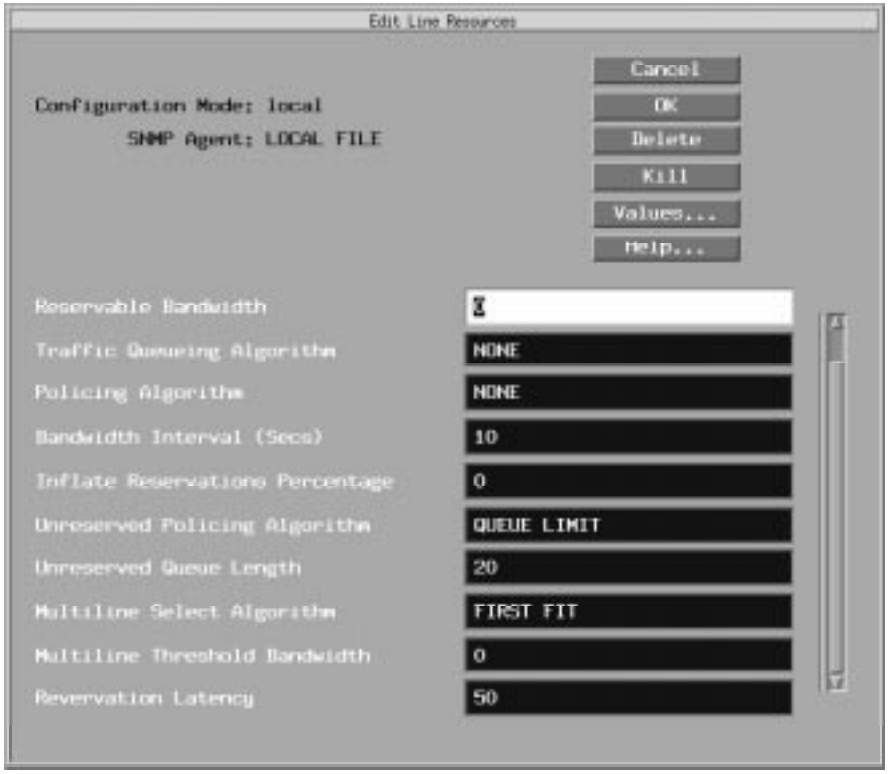

Figure 6-4. Edit Line Resources Window

Configuring the Resource Manager

When you activate the Resource Manager, you *must*

- Specify an estimated bandwidth value greater than 0.
- On a multiline circuit, edit the Multiline Select Algorithm and Multiline Threshold Bandwidth parameters.

You may also want to

- Modify or verify the default queuing of traffic for reserved bandwidth by setting the Traffic Queuing Algorithm, Policing Algorithm, Bandwidth Interval, and Inflate Reservations Percentage parameters.
- Modify or verify the default queuing of traffic for unreserved bandwidth by setting the Unreserved Policing Algorithm and Unreserved Queue Length parameters.
- Modify or verify the maximum latency for a reserved-flow packet by setting the Reservation Latency parameter.

See the applicable sections to configure Resource Manager parameters on an interface:

- Setting the Estimated Bandwidth
- Setting the Reservable Bandwidth
- Specifying the Traffic Queuing Algorithm
- Specifying the Policing Algorithm
- Setting the Bandwidth Interval
- Setting the Inflate Reservations Percentage
- Specifying the Unreserved Policing Algorithm
- Specifying the Unreserved Queue Length
- Specifying the Multiline Select Algorithm
- Setting the Multiline Threshold Bandwidth
- Setting the Reservation Latency

Setting the Estimated Bandwidth

To activate resource reservation, enter the portion of this line's bandwidth to make available for ST2 requests for guaranteed service.

Enter an estimated total bandwidth for this line, from 0 to 214748364 b/s. To enable line resource management, enter a value greater than 0.

For point-to-point lines, you can usually enter the total line speed.

For an Ethernet line, you must estimate a value, because shared-media lines may not have all of the bandwidth available. Base the estimate on line statistics, the number of connected workstations, or other site-specific information.

You can set the Estimated Bandwidth for this interface.

Site Manager: Estimated Bandwidth parameter: page A-27

Setting the Reservable Bandwidth

To enable ST2 reservable resources, specify the portion of this line's bandwidth to make available for ST2 requests for guaranteed service. The value can be any value from 0 to 214748364 b/s, and must be less than the value of the Estimated Bandwidth parameter.

Caution: Never make all available bandwidth reservable. Leave at least 15 percent of bandwidth available for network management, routing protocols, and other best-effort traffic.

You can set the Reservable Bandwidth for this interface.

Site Manager: Reservable Bandwidth parameter: page A-27

Specifying the Traffic Queuing Algorithm

By default, the Resource Manager uses best-effort scheduling for all reserved traffic. The resource reservation protocol (ST2) controls admission of flows to the network, but does not explicitly schedule each flow's packets.

You can select a priority queuing algorithm to schedule reserved traffic ahead of nonreserved traffic.

Set the Traffic Queuing Algorithm to None (best-effort scheduling for reserved traffic) or Priority (reserved traffic ahead of nonreserved) for this interface.

Site Manager: Traffic Queuing Algorithm parameter: page A-28

Specifying the Policing Algorithm

By default, the Resource Manager does not check ST2 packets against the flowspec (policing). This assumes that an upstream router is policing traffic, or the applications generating the reserved traffic consistently adhere to the flowspec and do not require policing.

When using the Leaky Bucket policing algorithm for reserved traffic, the Resource Manager makes sure that all ST2 packets using reserved bandwidth follow the flowspec that appears in the ST2 connect request. The Resource Manager discards any packets that do not adhere to the flowspec. Note that Leaky Bucket policing requires additional processing by the router.

For more information about Leaky Bucket policing, see “Specifying the Unreserved Policing Algorithm,” later in this chapter.

You can set the Policing Algorithm for this interface.

Site Manager: Policing Algorithm parameter: page A-28

Setting the Bandwidth Interval

By default, the Resource Manager measures instantaneous bandwidth over a 10 second interval. If 10 seconds is not sufficient, you can specify a different bandwidth interval for this interface, from 1 to 214748364 seconds.

Site Manager: Bandwidth Interval (Secs) parameter: page A-29

Setting the Inflate Reservations Percentage

By default, THE RESOURCE MANAGER does not add a safety buffer to each ST2 reservation on a line. To inflate reservations made on this line, enter a percent value to increase each bandwidth request.

Increase the value of this parameter if you notice that the Resource Manager is discarding packets because applications generating reserved traffic are exceeding their flowspecs.

Site Manager: Inflate Reservations Percentage parameter: page A-29

Specifying the Unreserved Policing Algorithm

The Resource Manager uses one of two policing algorithms for unreserved traffic:

- *Queue Limit* -- Restricts the number of buffers (packets) of unreserved traffic that the Resource Manager queues.

  This method of policing enables unreserved traffic to use available reserved bandwidth. Set the Unreserved Queue Length parameter to specify the maximum number of packets in the queue.

Note: If you enable priority queuing for this line, the router uses the priority queue parameters to perform Queue Limit policing. See *Configuring Traffic Filters and Protocol Prioritization* for information about priority queue parameters.

- *Leaky Bucket* -- Causes the router to actively police the unreserved traffic based on the unreserved bandwidth.

  This method does not allow unreserved traffic to take advantage of available reserved bandwidth.

You can set the Unreserved Policing Algorithm for this interface.

Site Manager: Unreserved Policing Algorithm parameter: page A-30

Specifying the Unreserved Queue Length

If the Unreserved Policing Algorithm parameter is set to Queue Limit, you can specify the maximum number of unreserved (best-effort) packets to be held in queue for transmission. After the queue length reaches this value, the router discards best-effort traffic when congestion occurs.

Note that Priority queuing limits, if configured, override the value of this parameter.

By default, the Resource Manager holds a maximum of 20 unreserved packets in queue for transmission. Change this value to adjust the queue length limit, a value from 0 to 214748364 packets (limited by available buffers).

Site Manager: Unreserved Queue Length parameter: page A-30

Specifying the Multiline Select Algorithm

If you configured the Resource Manager on a multiline circuit, you can choose one of two algorithms that determine how the Resource Manager selects which line to use for a new resource request:

- *First Fit* -- Always uses the first available line that can service reserved traffic requests
- *Round Robin* -- Rotates the use of lines available to service requests

All lines for a circuit must use the same algorithm. If any one line on a circuit specifies First Fit, all lines use the first-fit algorithm.

Site Manager: Multiline Select Algorithm parameter: page A-31

Setting the Multiline Threshold Bandwidth

When using the First Fit Multiline Select Algorithm (see the previous section, “Specifying the Multiline Select Algorithm”), you can configure a threshold of 0 to 214748364 b/s for the first available line.

By default, the threshold is set to 0; the Resource Manager uses the simple first-fit algorithm. If you select a value greater than 0, the Resource Manager still uses the first available line with reservable bandwidth to service requests, but moves to the next available line after reaching the configured threshold. When all lines are at their threshold, the Resource Manager resumes using the simple first-fit algorithm.

Set this parameter only if you have configured the Resource Manager on a multiline circuit and have set the Multiline Select Algorithm parameter to First Fit.

Site Manager: Multiline Threshold Bandwidth parameter: page A-31

Setting the Reservation Latency

By default, the maximum latency for a reserved flow packet is 50 milliseconds, limiting the amount of unreserved data that the link scheduler can transmit. When the data transmit ring reaches a size where the time to transmit the data is greater than the value of this parameter, no more unreserved data will be queued.

You can set the reservation latency from 0 to 214748364 milliseconds. Reduce the value of this parameter to obtain better delay characteristics for reserved flows, but note that overall throughput may decrease. Increase the default value to improve throughput, but note that reserved-flow delays may increase.

Site Manager: Reservation Latency parameter: page A-32

Disabling Line Resource Management

You can use the Configuration Manager to remove a line's resource reservation services or to delete the line resource record and completely disable the Resource Manager on a line.

Removing a Line's Reservations

To remove all outstanding reservations for a particular line:

1. **Start at the Configuration Manager window.**
2. **Click on the appropriate circuit connector.**

   The Edit Connector window appears (refer to Figure 6-2).
3. **Click on Edit Line Resources.**

   The Edit Line Resources window appears (refer to Figure 6-4).
4. **Click on Kill.**

   Site Manager displays the following message (Figure 6-5):

Figure 6-5. Removing a Line's Reserved Resources

5. **Click on OK.**

Deleting Resource Manager Services

To delete the line resource record and completely disable the Resource Manager on a circuit:

1. **Start at the Configuration Manager window.**
2. **Click on the appropriate circuit connector.**

The Edit Connector window appears (refer to Figure 6-2).

3. **Click on Edit Line Resources.**

   The Edit Line Resources window appears (refer to Figure 6-4).

4. **Click on Delete.**

   Site Manager displays a confirmation message for deleting the Resource Manager on this circuit (Figure 6-6):

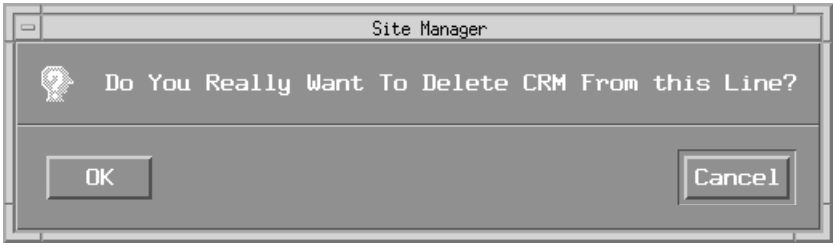

Figure 6-6. Deleting the Circuit's Resource Manager (CRM)

5. **Click on OK.**

   The Configuration Manager window appears.

The next time you select Edit Line Resources for this line in the Edit Connector window (refer to Figure 6-2), Site Manager will prompt you to re-create the line resource record. You can reconfigure resource reservation by completing the steps in "Starting the Resource Manager," earlier in this chapter.

Appendix A
Site Manager Multicast Parameters

For each line parameter associated with a multicast protocol or service, this appendix provides the Site Manager menu path to each parameter, information about default settings, valid parameter options, the parameter function, instructions for setting the parameter, and the MIB object ID. Find parameters in the following sections:

- DVMRP Parameters -- page A-1
- IGMP Parameters -- page A-12
- IP Configuration Parameters -- page A-17
- ST2 Parameters -- page A-19
- Resource Manager Parameters -- page A-27

DVMRP Parameters

This section describes the DVMRP global, circuit, and tunnel parameters.

DVMRP Global Parameters

Parameter: Enable

Path: Configuration Manager > Protocols > IP > Multicast > DVMRP > Global
Default: Enable
Options: Enable | Disable
Function: Enables and disables DVMRP support on the router.
Instructions: To disable DVMRP once you have configured it on the router, specify Disable.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.1.2

Parameter: Full Update Interval

Path: Configuration Manager > Protocols > IP > Multicast > DVMRP > Global
Default: 60
Options: 10 to 2000 seconds
Function: Specifies how often routing messages containing complete routing tables are sent.
Instructions: Determine the full update interval you require and specify a value.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.1.4

Parameter: Triggered Update Interval

Path: Configuration Manager > Protocols > IP > Multicast > DVMRP > Global
Default: 5
Options: 5 or more seconds
Function: Specifies the minimum amount of time between triggered updates.
Instructions: Triggered updates are sent in the period between full updates. Issuing a full update restarts the triggered update timer. Therefore, the triggered update interval you specify must be shorter than the full update interval you have specified with the Full Update Interval parameter.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.1.5

Parameter: Leaf Timeout

Path:	Configuration Manager > Protocols > IP > Multicast > DVMRP > Global
Default:	200
Options:	25 to 4000 seconds
Function:	Specifies a value for the Leaf Timeout timer.
Instructions:	Determine the timer interval you require and specify a value.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.12.1.6

Parameter: Neighbor Timeout

Path:	Configuration Manager > Protocols > IP > Multicast > DVMRP > Global
Default:	140
Options:	40 to 8000 seconds
Function:	Specifies how long a connection with a router neighbor is considered active without receiving a subsequent probe or report from the neighbor.
Instructions:	Determine a neighbor timeout period and specify a value.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.12.1.7

Parameter: Route Expiration Timeout

Path:	Configuration Manager > Protocols > IP > Multicast > DVMRP > Global
Default:	200
Options:	20 to 4000 seconds
Function:	Specifies how long a route is considered valid without the receipt of a subsequent update indicating that the route is reachable. This value represents the duration of time that this route will be used. Upon expiration of this timer, this route is advertised as unreachable until it is refreshed or deleted.
Instructions:	Enter a value that represents the duration of time this route will be used without being refreshed.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.12.1.8

Parameter: Garbage Timeout

Path: Configuration Manager > Protocols > IP > Multicast > DVMRP > Global

Default: 340

Options: 40 to 8000 seconds

Function: Specifies the duration of time that this route will be included in routing updates without the receipt of a subsequent update indicating that the route is reachable. The difference between this value and the Route Expiration Timeout value represents the duration of time that the route will be advertised as unreachable without subsequent refreshment.

Instructions: Enter a value that is greater than the value you specified for Route Expiration Timeout to allow for sufficient time for the route to be advertised as unreachable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.1.9

Parameter: Estimated Routes

Path: Configuration Manager > Protocols > IP > Multicast > DVMRP > Global

Default: 25

Options: An integer of 10 or greater

Function: Specifies the estimated number of routes.

Instructions: Enter a value that the router can use for preallocating routing tables. For an MBone deployment, a value of 3000 or higher is recommended. Note that routes are kept on a per-source-network basis, independent of multicast groups. This number must include a route for every network that is local to a circuit configured for multicasting. This allows the router to utilize memory efficiently. Exceeding this size during router operation will not cause an error but may cause the router to consume more memory than is required.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.1.10

Parameter: Neighbor Probe Interval

Path: Configuration Manager > Protocols > IP > Multicast > DVMRP > Global
Default: 10
Options: 5 to 30 seconds
Function: Specifies how often to send a probe on interfaces from which no neighbors have been heard.
Instructions: If your neighbor is running DVMRP *mrouted*, ensure that your probe interval value matches the value used by the neighbor.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.1.11

Parameter: Route Switch Timeout

Path: Configuration Manager > Protocols > IP > Multicast > DVMRP > Global
Default: 140
Options: 20 to 2000 seconds
Function: Specifies how long to wait, without receiving a subsequent route update from the original neighbor, before switching to a different neighbor advertising equal cost for this route.
Instructions: If your neighbor is running DVMRP *mrouted*, the recommended value is 140 seconds.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.1.12

Parameter: Debug Level

Path: Configuration Manager > Protocols > IP > Multicast > DVMRP > Global
Default: 0
Options: 0 or a debug level
Function: Turns the DVMRP log on or off for DVMRP debugging messages and specifies the level of debug messages.
Instructions: By default (0), the log is turned off. Specify a level only when directed by Customer Support personnel to investigate a problem.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.1.14

Parameter: Pruning Enable

Path: Configuration Manager > Protocols > IP > Multicast > DVMRP > Global
Default: Enable
Options: Enable | Disable
Function: Enables or disables pruning functionality on the router.
Instructions: DVMRP performs route pruning by default. If you want to disable this function on the router, select Disable.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.1.15

Parameter: Fragmented MTU Threshold

Path: Configuration Manager > Protocols > IP > Multicast > DVMRP > Global
Default: 1514
Options: 910 to 1514 bytes
Function: Specifies the MTU size. The maximum (and default) size is the CSMACD_MTU size. The minimum is the X25_DDN_MTU size.
Instructions: DVMRP compares datagrams received by the router with the threshold value you specify. If the size of the datagram exceeds the threshold size, IP fragments the datagram. DVMRP makes this decision based on the comparison between the outgoing interface's MTU and either this threshold value, if you configure it, or the incoming interface's MTU.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.1.16

Parameter: Max Routes

Path: Configuration Manager > Protocols > IP > Multicast > DVMRP > Global
Default: 0
Options: 0 or an integer
Function: Specifies the number of routes that DVMRP can learn per slot. This parameter limits the number of routes that can be stored in the routing table.
Instructions: If you want DVMRP to store all learned routes in the routing table, use the default, 0. If you specify a maximum number of routes, you must include a route for every local network that has a circuit configured for multicasting.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.1.17

DVMRP Circuit Parameters

Parameter: Enable

Path: Configuration Manager > Protocols > IP > Multicast > DVMRP > Circuit
Default: Enable
Options: Enable │ Disable
Function: Enables or disables DVMRP on this circuit.
Instructions: If you have configured DVMRP on this circuit, enter Disable to disable it.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.2.1.2

Parameter: Route Enable

Path: Configuration Manager > Protocols > IP > Multicast > DVMRP > Circuit
Default: Enable
Options: Enable │ Disable
Function: Enables or disables this circuit for routing.
Instructions: Specify Enable if you want this circuit to be used to propagate routing information, and if you want information about the source network associated with this circuit incorporated into routing updates. Specify Enable if you want multicast datagrams to be forwarded on this circuit in “native mode” -- that is, as multicast datagrams. You can configure tunnels on this circuit.

Specify Disable if you want this circuit to exist only to support unicast tunnels. If you specify Disable, all other DVMRP circuit parameters are ignored. The source network associated with this circuit is not incorporated into the routing updates.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.2.1.5

Parameter: Metric

Path: Configuration Manager > Protocols > IP > Multicast > DVMRP > Circuit
Default: 1
Options: 1 to 31
Function: Specifies the cost of this interface.
Instructions: Determine the cost that you want to assign to this hop and enter a value. We recommend the following values: for a LAN, or tunnel across a single LAN, 1; for a multihop tunnel, 2 or 3; for a serial link, or tunnel across a serial link, 1; for a backup tunnel, the primary tunnel metric + 1.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.2.1.6

Parameter: Threshold

Path: Configuration Manager > Protocols > IP > Multicast > DVMRP > Circuit
Default: 1 hop
Options: 1 to 254 hops
Function: Specifies a TTL value for the interface. This value is the minimum IP TTL required for a multicast datagram to be forwarded out this interface.
Instructions: Use this parameter to control the scope of the datagrams. If the IP TTL is less than the threshold value you specify, the datagram is dropped by the router.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.2.1.7

Parameter: Forward Cache Size

Path: Configuration Manager > Protocols > IP > Multicast > DVMRP > Circuit
Default: 32
Options: 32 to 512 entries
Function: Specifies the maximum number of entries allowed in the forwarding table associated with this interface.
Instructions: When configuring a cache size, you must also keep in mind the TTL value for entries. If you specify a large cache size, a larger TTL value is recommended. For a smaller cache, a shorter TTL for cache entries is recommended.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.2.1.14

Parameter:	**Forward Cache TTL**
Path:	Configuration Manager > Protocols > IP > Multicast > DVMRP > Circuit
Default:	300
Options:	300 to 86400 seconds
Function:	Specifies the TTL for an entry in the forwarding table.
Instructions:	If your neighbor is running DVMRP *mrouted*, we recommend a TTL value of 300 seconds.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.12.2.1.15

Parameter:	**Advertise Self**
Path:	Configuration Manager > Protocols > IP > Multicast > DVMRP > Circuit
Default:	Advertise
Options:	Advertise | Do Not Advertise
Function:	Specifies whether the router advertises its own local networks over this interface.
Instructions:	If you do not want routes advertised over a particular interface, set that interface to Do Not Advertise.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.12.2.1.16

DVMRP Tunnel Parameters

Parameter: Enable

Path: Configuration Manager > Protocols > IP > Multicast > DVMRP > Tunnel
Default: Enable
Options: Enable | Disable
Function: Enables or disables this tunnel interface.
Instructions: If you have configured this tunnel, specify Disable to disable the tunnel.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.3.1.2

Parameter: Encapsulation Mode

Path: Configuration Manager > Protocols > IP > Multicast > DVMRP > Tunnel
Default: IPINIP
Options: IPINIP | LSSR
Function: Specifies whether tunneled datagrams are encapsulated within an IP datagram or loosely encapsulated using the LSSR option.
Instructions: See RFC 1075 for information about the LSSR option, which is provided for backward compatibility.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.3.1.6

Parameter: Metric

Path: Configuration Manager > Protocols > IP > Multicast > DVMRP > Tunnel
Default: 1
Options: 1 to 31
Function: Specifies the cost of this tunnel.
Instructions: Determine the cost you want to assign to this hop and enter a value.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.3.1.7

Parameter: Threshold

Path: Configuration Manager > Protocols > IP > Multicast > DVMRP > Tunnel
Default: 1
Options: 1 to 254 hops
Function: Specifies a TTL value for the tunnel. This value is the minimum IP TTL required for a multicast datagram to be forwarded out this tunnel.
Instructions: Use this parameter to control the scope of the datagrams. If the IP TTL is less than the threshold value you specify, the datagram is dropped by the router.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.3.1.8

Parameter: Forward Cache Size

Path: Configuration Manager > Protocols > IP > Multicast > DVMRP > Tunnel
Default: 32
Options: 32 to 512 entries
Function: Specifies the maximum number of entries allowed in the forwarding table associated with this tunnel interface.
Instructions: When configuring a cache size, you must also keep in mind the TTL value for entries. If you specify a large cache size, a larger TTL value is recommended. For a smaller cache, a shorter TTL for cache entries is recommended.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.3.1.16

Parameter: Forward Cache TTL

Path: Configuration Manager > Protocols > IP > Multicast > DVMRP > Tunnel
Default: 300
Options: 300 to 86400 seconds
Function: Specifies the TTL for an entry in the forwarding table.
Instructions: Select an appropriate value for your configuration.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.3.1.17

Parameter: Local IP Address

Path: Configuration Manager > Protocols > IP > Multicast > DVMRP > Tunnel > Click on Add

Default: Null

Options: The unicast IP address of an interface on a circuit supporting multicasting on the local router

Function: Identifies the local end of the tunnel. To identify a unicast tunnel, you must supply the unicast IP address of both ends of the tunnel: the local interface and the remote interface.

Instructions: Use this parameter to enter the local IP address.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.3.1.4

Parameter: Remote IP address

Path: Configuration Manager > Protocols > IP > Multicast > DVMRP > Tunnel > Click on Add

Default: Null

Options: The unicast IP address of an interface supporting multicasting on a neighboring router

Function: Identifies the remote end of the tunnel. To identify a unicast tunnel, you must supply the unicast IP address of both ends of the tunnel: the local interface and the remote interface.

Instructions: Use this parameter to enter the remote IP address.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.12.3.1.5

IGMP Parameters

This section describes the IGMP global configuration, static host, and entry interface parameters.

IGMP Global Configuration Parameters

Parameter: Enable

Path: Configuration Manager > Protocols > IP > Multicast > IGMP > Global
Default: Enable
Options: Enable | Disable
Function: Enables or disables this IGMP record.
Instructions: If you have configured IGMP on this router, use this parameter to disable it.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.1.2

Parameter: Estimated Groups

Path: Configuration Manager > Protocols > IP > Multicast > IGMP > Global
Default: 20
Options: 5 to 65535 groups
Function: Specifies the estimated number of groups that will be simultaneously active for this router.
Instructions: Determine the approximate number of groups and enter the value. This is to allow the router to utilize memory efficiently. Exceeding this size during router operation will not cause an error but may cause the router to consume more memory than required. The following groups are not maintained by IGMP; you do not need to include them in the count: 224.0.0.1, 224.0.0.4, 224.0.0.5, and 224.0.0.6.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.1.4

Parameter: Version Threshold Time

Path: Configuration Manager > Protocols > IP > Multicast > IGMP > Global
Default: 540
Options: 1 to 65535 seconds
Function: The number of seconds that can elapse after IGMP detects a Version 1 query before IGMP tries to become the designated querier.
Instructions: The value you specify should be greater than the Version 1 query rate of all IGMP speakers on all networks directly connected to the router.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.1.5

Parameter: **Debug**

Path: Configuration Manager > Protocols > IP > Multicast > IGMP > Global

Default: None

Options: Receive │ Send │ Other

Function: Causes IGMP to generate the specified log messages.

Instructions: Specify zero or more options. Set this parameter to Receive to log messages received. Set the parameter to Send to log messages sent. Set the parameter to Other to log other types of IGMP messages.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.1.6

IGMP Static Host Parameters

Parameter: **Static Group CCT**

Path: Configuration Manager > Protocols > IP > Multicast > IGMP > Global

Default: None

Options: A circuit number

Function: Specifies the circuit number for the local network on which the group member resides.

Instructions: Use the Static Group CCT parameter -- along with the Static Group Address and Static Group Prefix parameters -- to statically register the network on which the multicast group member resides.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.4.1.2

Parameter: **Static Group Address**

Path: Configuration Manager > Protocols > IP > Multicast > IGMP > Global

Default: None

Options: A multicast address

Function: Specifies the multicast address for the group of which the host is a member.

Instructions: Use the Static Group Address parameter -- along with the Static Group CCT and Static Group Prefix parameters -- to statically register the network on which the multicast group member resides.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.4.1.3

Parameter:	**Static Group Prefix**
Path:	Configuration Manager > Protocols > IP > Multicast > IGMP > Global
Default:	None
Options:	An address prefix
Function:	Specifies the prefix of the multicast group address.
Instructions:	Use the Static Group Prefix parameter -- along with the Static Group CCT and Static Group Address parameters -- to statically register the network on which the multicast group member resides.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.13.4.1.4

IGMP Entry Interface Parameters

Parameter:	**Enable**
Path:	Configuration Manager > Protocols > IP > Multicast > IGMP > Entry
Default:	Enable
Options:	Enable | Disable
Function:	Indicates whether this IGMP interface record is enabled or disabled.
Instructions:	If you have configured IGMP on this interface, use this parameter to disable it.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.13.2.1.2

Parameter: Interface Query Rate

Path: Configuration Manager > Protocols > IP > Multicast > IGMP > Entry

Default: 120

Options: 0 to 4096 seconds

Function: Specifies how often the router sends group membership queries on the interface.

Instructions: If there are no multicast hosts on this circuit, set the parameter to 0 to disable queries. Specifying 0 affects queries only. The router still forwards multicast datagrams on this circuit. If another IGMP router on this network has taken on the query role, this router will not send queries unless it has not heard of any queries within the number of seconds specified by the Designated Router Timeout parameter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.2.1.5

Parameter: Interface Membership Timeout

Path: Configuration Manager > Protocols > IP > Multicast > IGMP > Entry

Default: 260

Options: 30 to 8192 seconds

Function: Specifies the amount of time that a local group membership is valid without the receipt of a subsequent report for that group.

Instructions: The suggested value is (2 * Query Rate) + 20.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.2.1.6

Parameter: Designated Router Timeout

Path: Configuration Manager > Protocols > IP > Multicast > IGMP > Entry

Default: 140

Options: 10 to 8192 seconds

Function: Specifies the amount of time that can elapse after the last host query message before the IGMP designated router is considered down.

Instructions: The value you specify should be greater than the query rate of all IGMP routers on the network.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.2.1.7

Parameter: **Max Host Response Time**

Path: Configuration Manager > Protocols > IP > Multicast > IGMP > Entry

Default: 100

Options: 1 to 100 tenths of a second

Function: Specifies a maximum value for the amount of time that a host must wait before responding to a query. IGMP places this value in the code field of an IGMP query.

Instructions: Specify a maximum response time for this interface.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.13.2.1.15

IP Configuration Parameters

Parameter: **IP Address**

Path: Select IP from the Select Protocols window and click on OK.

Default: None

Options: 0.0.0.0 or any valid IP address

Function: Assigns a 32-bit IP address to the interface.

Instructions: Enter the IP address of the interface in dotted-decimal notation. Enter 0.0.0.0 to configure an unnumbered interface on the circuit.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.1.4.1.4

Parameter: **Subnet Mask**

Path: Select IP from the Select Protocols window and click on OK.

Default: None

Options: The Configuration Manager automatically calculates an appropriate subnet mask, depending on the class of the network to which the interface connects. However, you can change the subnet mask with this parameter.

Function: Specifies the network and subnetwork portion of the 32-bit IP address.

Instructions: Either accept the assigned subnet mask or enter another subnet mask in dotted-decimal notation. Enter 0.0.0.0 if you are configuring an unnumbered interface on the circuit.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.1.4.1.6

Parameter: Transmit Bcast Addr

Path: Select IP from the Select Protocols window and click on OK.

Default: 0.0.0.0

Options: 0.0.0.0 or any valid IP broadcast address

Function: Specifies the broadcast address that this IP subnet uses to broadcast packets. Accepting 0.0.0.0 for this parameter specifies that the IP router will use a broadcast address with a host portion of all 1s. Accepting 0.0.0.0 does not configure the router to use the address 0.0.0.0 to broadcast packets. For example, if you have IP address 123.1.1.1 and a subnet mask of 255.255.255.0, accepting the default value 0.0.0.0 configures the IP router to use the address 123.1.1.255 to broadcast packets. To set the explicit broadcast address of all 1s, enter 255.255.255.255 for this parameter.

Instructions: Accept the default, 0.0.0.0, unless the calculated broadcast address (host portion) of all 1s is not adequate. If this is the case, then enter the appropriate IP broadcast address in dotted-decimal notation. If you set the IP Address parameter to 0.0.0.0 (to configure an unnumbered interface), Site Manager automatically sets this parameter to 255.255.255.255.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.1.4.1.8

Parameter: UnNumbered Assoc Address

Path: Select IP from the Select Protocols window and click on OK.

Default: None

Options: Any valid IP address

Function: Specifies an address that IP uses when sourcing a packet. RIP uses this address to make decisions about advertising subnets over the unnumbered interface. RIP advertises subnets over the unnumbered interface if the subnets have the same mask as the associated address.

Instructions: Specify the address of any numbered interface on the router. If you are running RIP over the unnumbered interface and if you are using a subnet address as the associated address, the local and remote associated addresses should have the same network number. If you configure local and remote associated addresses using different network numbers, you must use RIP2 mode.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.2.1.4.1.110

ST2 Parameters

This section describes the ST2 global, interface, and Neighbors Forwarding Table parameters.

ST2 Global Parameters

Parameter: Enable

Path: Configuration Manager > Protocols > IP > ST2 > Global
Default: Enable
Options: Enable | Disable
Function: Determines whether ST2 is enabled on the slot.
Instructions: By default, the router starts ST2 on the slot when you configure an ST2 interface on a circuit. If you do not want ST2 to be started on the slot, select Disable.
MIB Object ID: 1.3.6.1.4.1.18.3.5.16.1.2.1.2

Parameter: Tunnelling Capability

Path: Configuration Manager > Protocols > IP > ST2 > Global
Default: No
Options: Yes | No
Function: Specifies whether ST2 can use a tunnel to establish a neighbor-to-neighbor connection.
Instructions: By default, ST2 does not have tunneling capability. If your network requires the use of tunnels, select Yes.
MIB Object ID: 1.3.6.1.4.1.18.3.5.16.1.2.1.5

Parameter: **Tunneling Enable**

Path: Configuration Manager > Protocols > IP > ST2 > Global

Default: Disable

Options: Enable │ Disable

Function: Enables and disables tunneling on a router that has tunneling capability.

Instructions: If you select Yes for the Tunneling Capability parameter, use this parameter to enable and disable that feature on the router.

MIB Object ID: 1.3.6.1.4.1.18.3.5.16.1.2.1.6

ST2 Interface Parameters

Parameter: **Enable**

Path: Configuration Manager > Protocols > IP > ST2 > Interfaces

Default: Enable

Options: Enable │ Disable

Function: Enables and disables ST2 on this interface.

Instructions: By default, the router enables ST2 when you add the ST2 protocol to the circuit. If you want to disable ST2 on the interface, use this parameter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.16.1.2.2.1.2

Parameter: **IP Address**

Path: Configuration Manager > Protocols > IP > ST2 > Interfaces

Default: None

Options: Any valid IP address

Function: Specifies the IP address of this ST2 interface.

Instructions: Supply a unique IP address in dotted decimal notation.

MIB Object ID: 1.3.6.1.4.1.18.3.5.16.1.2.2.1.6

Parameter: Accept Time Out

Path: Configuration Manager > Protocols > IP > ST2 > Interfaces
Default: 10
Options: 1 to 999 seconds
Function: Specifies the time between ST2 accept message retries on this interface.
Instructions: Use the default unless the application requires otherwise.
MIB Object ID: 1.3.6.1.4.1.18.3.5.16.1.2.2.1.7

Parameter: Accept Retry

Path: Configuration Manager > Protocols > IP > ST2 > Interfaces
Default: 3
Options: 1 to 100 retries
Function: Specifies the maximum retry count for accept messages on this interface.
Instructions: Use the default unless the application requires otherwise.
MIB Object ID: 1.3.6.1.4.1.18.3.5.16.1.2.2.1.8

Parameter: Connect Time Out

Path: Configuration Manager > Protocols > IP > ST2 > Interfaces
Default: 10
Options: 1 to 999 seconds
Function: Specifies the time between ST2 connect message retries on this interface.
Instructions: Use the default unless the application requires otherwise.
MIB Object ID: 1.3.6.1.4.1.18.3.5.16.1.2.2.1.9

Parameter: Connect Retry

Path: Configuration Manager > Protocols > IP > ST2 > Interfaces
Default: 5
Options: 1 to 100 retries
Function: Specifies the maximum retry count for connect messages on this interface.
Instructions: Use the default unless the application requires otherwise.
MIB Object ID: 1.3.6.1.4.1.18.3.5.16.1.2.2.1.10

Parameter: Disconnect Time Out

Path: Configuration Manager > Protocols > IP > ST2 > Interfaces
Default: 10
Options: 1 to 999 seconds
Function: Specifies the time between ST2 disconnect message retries on this interface.
Instructions: Use the default unless the application requires otherwise.
MIB Object ID: 1.3.6.1.4.1.18.3.5.16.1.2.2.1.11

Parameter: Disconnect Retry

Path: Configuration Manager > Protocols > IP > ST2 > Interfaces
Default: 3
Options: 1 to 100 retries
Function: Specifies the maximum retry count for disconnect messages on this interface.
Instructions: Use the default unless the application requires otherwise.
MIB Object ID: 1.3.6.1.4.1.18.3.5.16.1.2.2.1.12

Parameter: HID Change Time Out

Path: Configuration Manager > Protocols > IP > ST2 > Interfaces
Default: 10
Options: 1 to 999 seconds
Function: Specifies the time between ST2 HID change message retries on this interface.
Instructions: Use the default unless the application requires otherwise.
MIB Object ID: 1.3.6.1.4.1.18.3.5.16.1.2.2.1.13

Parameter: HID Change Retry

Path: Configuration Manager > Protocols > IP > ST2 > Interfaces
Default: 3
Options: 1 to 100 retries
Function: Specifies the maximum retry count for HID change messages on this interface.
Instructions: Use the default unless the application requires otherwise.
MIB Object ID: 1.3.6.1.4.1.18.3.5.16.1.2.2.1.14

Parameter: Refuse Time Out

Path: Configuration Manager > Protocols > IP > ST2 > Interfaces
Default: 10
Options: 1 to 999 seconds
Function: Specifies the time between ST2 refuse message retries on this interface.
Instructions: Use the default unless the application requires otherwise.
MIB Object ID: 1.3.6.1.4.1.18.3.5.16.1.2.2.1.15

Parameter: Refuse Retry

Path: Configuration Manager > Protocols > IP > ST2 > Interfaces
Default: 3
Options: 1 to 100 retries
Function: Specifies the maximum retry count for refuse messages on this interface.
Instructions: Use the default unless the application requires otherwise.
MIB Object ID: 1.3.6.1.4.1.18.3.5.16.1.2.2.1.16

Parameter: Hello Time Out

Path: Configuration Manager > Protocols > IP > ST2 > Interfaces
Default: 10
Options: 1 to 100 seconds
Function: Specifies the time between ST2 hello message retries on this interface.
Instructions: Use the default unless the application requires otherwise.
MIB Object ID: 1.3.6.1.4.1.18.3.5.16.1.2.2.1.17

Parameter: Hello Retry

Path: Configuration Manager > Protocols > IP > ST2 > Interfaces
Default: 5
Options: 1 to 100 retries
Function: Specifies the maximum retry count for hello messages on this interface.
Instructions: Use the default unless the application requires otherwise.
MIB Object ID: 1.3.6.1.4.1.18.3.5.16.1.2.2.1.18

ST2 Neighbors Forwarding Table Parameters

Parameter: Enable

Path: Configuration Manager > Protocols > IP > ST2 > Neighbors
Default: Enable
Options: Enable | Disable
Function: Specifies whether the record for this neighbor is active.
Instructions: Use this parameter to disable a configured neighbor.
MIB Object ID: 1.3.6.1.4.1.18.3.5.16.1.2.3.1.2

Parameter: **Route Exploration Capability**

Path: Configuration Manager > Protocols > IP > ST2 > Neighbors
Default: No
Options: Yes | No
Function: Specifies whether the neighbor is capable of route exploration.
Instructions: Determine this characteristic of the ST2 neighbor and supply the proper value.
MIB Object ID: 1.3.6.1.4.1.18.3.5.16.1.2.3.1.2.4

Parameter: **Hello Protocol**

Path: Configuration Manager > Protocols > IP > ST2 > Neighbors
Default: Enable
Options: Enable | Hello When Stream Active | Disable
Function: Specifies whether the router should send hello messages to the neighbor. The parameter also specifies the type of hello procedure.
Instructions: Select Enable to use the normal Bay Networks hello procedure. Select Hello When Stream Active to use the hello procedure only when a stream is running to a neighbor. Select Disable to disable the feature on the interface.
MIB Object ID: 1.3.6.1.4.1.18.3.5.16.1.2.3.1.2.5

Parameter: **Neighbor Type**

Path: Configuration Manager > Protocols > IP > ST2 > Neighbors
Default: Local
Options: Local | Tunnel
Function: Specifies the type of connection to this neighbor.
Instructions: Set this parameter to Tunnel if the router is connected to the neighbor via an ST2 tunnel.
MIB Object ID: 1.3.6.1.4.1.18.3.5.16.1.2.3.1.2.6

Parameter: Neighbor Priority Level

Path: Configuration Manager > Protocols > IP > ST2 > Neighbors
Default: 8
Options: 1 to 16
Function: Assigns a priority value to the neighbor.
Instructions: If you enter multiple ST2 route exploration neighbors in the forwarding table, use this parameter to rank them. First choice is the neighbor with the lowest value.
MIB Object ID: 1.3.6.1.4.1.18.3.5.16.1.2.3.1.2.7

Parameter: Next Hop IP Address

Path: Configuration Manager > Protocols > IP > ST2 > Neighbors
Default: None
Options: A valid IP address
Function: Specifies the IP address of the next-hop router or host.
Instructions: Set to the IP address of the neighbor (router or host).
MIB Object ID: 1.3.6.1.4.1.18.3.5.16.1.2.3.1.2.3

Resource Manager Parameters

Parameter: Estimated Bandwidth

Path: Configuration Manager > XCVR, HSSI, MCT1, or COM Connector configured for the ST2 protocol > Edit Line Resources > Edit Line Resources

Default: 0

Options: 0 to 214748364 b/s

Function: Specifies the estimated usable bandwidth for this line.

Instructions: Enter the estimated total bandwidth for this line in bits/s. To enable line resource management, enter a value greater than zero. For point-to-point lines, you can usually enter the total line speed.

For an Ethernet line, you must estimate a value, because shared-media lines may not have all of the bandwidth available. You can base the estimate on line statistics, the number of connected workstations, or other site-specific information.

MIB Object ID: 1.3.6.1.4.1.18.3.5.16.2.1.3.1.3

Parameter: Reservable Bandwidth

Path: XCVR, HSSI, MCT1, or COM Connector configured for the ST2 protocol > Edit Line Resources > Edit Line Resources

Default: 0

Options: 0 to 214748364 b/s

Function: Specifies the reservable bandwidth for this line.

Instructions: To enable ST2 reservable resources, enter the portion of this line's bandwidth that you want to make available for ST2 requests for guaranteed service. The value must be greater than 0 and less than the value of the Estimated Bandwidth parameter. Do not make all available bandwidth reservable; leave at least 15 percent for network management and routing protocols.

MIB Object ID: 1.3.6.1.4.1.18.3.5.16.2.1.3.1.4

Parameter: Traffic Queuing Algorithm

Path: Configuration Manager > XCVR, HSSI, MCT1, or COM Connector configured for the ST2 protocol > Edit Line Resources > Edit Line Resources

Default: None

Options: None | Priority

Function: Specifies the queuing algorithm for all reserved traffic.

Instructions: Select None to use best-effort scheduling. Use best-effort scheduling if you want to use the resource reservation protocol (ST2) to control admission of flows to the network, but do not want to explicitly schedule each flow's packets.

MIB Object ID: 1.3.6.1.4.1.18.3.5.16.2.1.3.1.5

Parameter: Policing Algorithm

Path: Configuration Manager > XCVR, HSSI, MCT1, or COM Connector configured for the ST2 protocol > Edit Line Resources > Edit Line Resources

Default: None

Options: None | Leaky Bucket

Function: Specifies whether or not to use the Leaky Bucket policing algorithm for reserved traffic. With Leaky Bucket policing, the Resource Manager makes sure that all ST2 packets using reserved bandwidth follow the flowspec that appears in the ST2 connect request. The Resource Manager discards any packets that do not adhere to the flowspec. Note that such policing requires additional processing by the router.

Instructions: Select None to bypass policing if an upstream router is policing traffic, or if the applications generating the reserved traffic consistently adhere to the flowspec and do not require policing.

Enter Leaky Bucket to apply a Leaky Bucket policing algorithm to reserved traffic.

MIB Object ID: 1.3.6.1.4.1.18.3.5.16.2.1.3.1.6

Parameter: Bandwidth Interval (Secs)

Path: Configuration Manager > XCVR, HSSI, MCT1, or COM Connector configured for the ST2 protocol > Edit Line Resources > Edit Line Resources

Default: 10

Options: 1 to 214748364 seconds

Function: Specifies the interval over which the Resource Manager measures instantaneous bandwidth.

Instructions: Enter a time interval in seconds if the default value of 10 seconds is not sufficient.

MIB Object ID: 1.3.6.1.4.1.18.3.5.16.2.1.3.1.7

Parameter: Inflate Reservations Percentage

Path: Configuration Manager > XCVR, HSSI, MCT1, or COM Connector configured for the ST2 protocol > Edit Line Resources > Edit Line Resources

Default: 0

Options: 0 to 100 percent

Function: Specifies that the Resource Manager adds a safety buffer to each ST2 reservation on this line by increasing bandwidth requests by a specified percentage.

Instructions: To inflate reservations made on this line, enter a percent value to increase each bandwidth request. Increase the value of this parameter if you notice that the Resource Manager is discarding packets because applications generating reserved traffic are exceeding their flowspecs.

MIB Object ID: 1.3.6.1.4.1.18.3.5.16.2.1.3.1.8

Parameter: Unreserved Policing Algorithm

Path: Configuration Manager > XCVR, HSSI, MCT1, or COM Connector configured for the ST2 protocol > Edit Line Resources > Edit Line Resources

Default: Queue Limit

Options: Queue Limit | Leaky Bucket

Function: Specifies the policing algorithm for unreserved traffic.

Instructions: Select the Queue Limit option to restrict the number of buffers (packets) of unreserved traffic that the Resource Manager queues. This method of policing enables unreserved traffic to use available reserved bandwidth. The Unreserved Queue Length parameter specifies the maximum number of packets in the queue.

Select the Leaky Bucket option to cause the router to actively police the unreserved traffic based on the unreserved bandwidth. This method does not allow unreserved traffic to take advantage of available reserved bandwidth.

If you enable priority queuing for this line, the router uses the priority queue parameters to perform Queue Limit policing. See *Configuring Traffic Filters and Protocol Prioritization* for information about priority queue parameters.

MIB Object ID: 1.3.6.1.4.1.18.3.5.16.2.1.3.1.9

Parameter: Unreserved Queue Length

Path: Configuration Manager > XCVR, HSSI, MCT1, or COM Connector configured for the ST2 protocol > Edit Line Resources > Edit Line Resources

Default: 20

Options: 0 to 214748364 packets (limited by available buffers)

Function: If the Unreserved Policing Algorithm parameter is set to Queue Limit, this parameter specifies the maximum number of unreserved (best-effort) packets to be held in queue for transmission.

After the queue length reaches this value, the router discards best-effort traffic when congestion occurs.

Priority queuing limits, if configured, override the value of this parameter.

Instructions: Change this value to adjust the queue length limit.

MIB Object ID: 1.3.6.1.4.1.18.3.5.16.2.1.3.1.10

Parameter: **Multiline Select Algorithm**

Path: Configuration Manager > XCVR, HSSI, MCT1, or COM Connector configured for the ST2 protocol > Edit Line Resources > Edit Line Resources

Default: First Fit

Options: First Fit | Round Robin

Function: Specifies how the Resource Manager selects which line to use for a new resource request, if you have the Resource Manager configured on a multiline circuit.

Instructions: Set this parameter only if you configured the Resource Manager on a multiline circuit.

Select First Fit to always use the first available line that can service reserved traffic requests. Select Round Robin to rotate the use of lines available to service requests. All lines for a circuit must use the same algorithm. If any one line on a circuit specifies First Fit, all lines use the first-fit algorithm.

MIB Object ID: 1.3.6.1.4.1.18.3.5.16.2.1.3.1.11

Parameter: **Multiline Threshold Bandwidth**

Path: Configuration Manager > XCVR, HSSI, MCT1, or COM Connector configured for the ST2 protocol > Edit Line Resources > Edit Line Resources

Default: 0

Options: 0 to 214748364 b/s

Function: Specifies how the first-fit algorithm works, providing you set the Multiline Select Algorithm parameter to First Fit. If you accept the default value, the Resource Manager uses the simple first-fit algorithm. If you select a value greater than 0, the Resource Manager still uses the first available line with reservable bandwidth to service requests, but moves to the next available line after reaching the configured threshold. When all lines are at their threshold, the Resource Manager resumes using the simple first-fit algorithm.

Instructions: Set this parameter only if you have configured the Resource Manager on a multiline circuit and have set the Multiline Select Algorithm parameter to First Fit.

Accept the default or enter a number less than the value of the Reservable Bandwidth parameter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.16.2.1.3.1.12

Parameter:	**Reservation Latency**
Path:	Configuration Manager > XCVR, HSSI, MCT1, or COM Connector configured for the ST2 protocol > Edit Line Resources > Edit Line Resources
Default:	50
Options:	0 to 214748364 milliseconds
Function:	Specifies the maximum latency for a reserved flow packet, limiting the amount of unreserved data that the link scheduler can transmit. When the data transmit ring reaches a size where the time to transmit the data is greater than the value of this parameter, no more unreserved data will be queued.
Instructions:	Reduce the value of this parameter to obtain better delay characteristics for reserved flows, but note that overall throughput may decrease. Increase the default value to improve throughput, but note that reserved-flow delays may increase.
MIB Object ID:	1.3.6.1.4.1.18.3.5.16.2.1.3.1.13

Index

A

agent, defined, 5-2

B

Bay Networks Press, xxiv

Bay Networks World Wide Web page, xxv

C

connect request
- forwarding downstream, 5-10
- receiving from upstream, 5-7

customer support
- programs, xxiv
- technical response centers, xxv

D

data packets, forwarding downstream, 5-12

deleting
- line reservations, 6-12
- LRM services, 6-12

DVMRP parameters
- circuit
  - Advertise Self, A-9
  - Enable, A-7
  - Forward Cache Size, A-8, A-11
  - Metric, A-8
  - Route Enable, A-7
  - Threshold, A-8
- global
  - Debug Level, A-5
  - Enable, A-2
  - Estimated Routes, A-4
  - Fragmented MTU Threshold, A-6
  - Full Update Rate, A-2
  - Garbage Timeout, A-4
  - Leaf Timeout, A-3
  - Neighbor Probe Interval, A-5
  - Neighbor Timeout, A-3
  - Pruning Enable, A-6
  - Route Expiration Timeout, A-3
  - Route Switch Timeout, A-5
  - Triggered Update Rate, A-2
- tunnel
  - Enable, A-10
  - Encapsulation Mode, A-10
  - Local IP Address, A-12
  - Metric, A-10
  - Remote IP address, A-12
  - Threshold, A-11

E

exploratory routing, defined, 5-10

F

flowspec (flow specification), 5-4, 6-3

H

hop identifier (HID), 5-4

host agent, defined, 5-2

I

IGMP (Internet Group Management Protocol), 1-1

IGMP parameters
- entry
  - Designated Router Timeout, A-16
  - Enable, A-15
  - Interface Membership Timeout, A-16
- global
  - Enable, A-13
  - Estimated Groups, A-13

intermediate agent, defined, 5-2

Internet Group Management Protocol (IGMP), 1-1

internet, relationship to ST2, 5-2

IP parameters
- IP Address, A-17
- Subnet Mask, A-17
- Transmit Bcast Addr, A-18

IP-inherited routing, 5-9

L

Line Resource Manager (LRM)
- configuring, 6-3 to 6-13
- disabling, 6-12
- line resource record, 6-12
- overview, 6-2
- parameters
  - Bandwidth Interval (Secs), 6-8, A-29
  - Estimated Bandwidth, 6-7, A-27
  - Inflate Reservations Percentage, 6-9, A-29
  - Multiline Select Algorithm, 6-10, A-31
  - Multiline Threshold Bandwidth, 6-11, A-31
  - Policing Algorithm, 6-8, A-28
  - Reservable Bandwidth, 6-7, A-27
  - Reservation Latency, 6-11, A-32
  - Traffic Queuing Algorithm, 6-8, A-28
  - Unreserved Policing Algorithm, 6-9, A-30
  - Unreserved Queue Length, 6-10, A-30

M

multicasting
- aging a route, 4-9
- comparing routes, 4-6
- creating a shortest path tree, 4-6
- IGMP, 1-1
- leaf network, 4-7
- threshold, 4-14
- tunnel, 4-2

N

neighbor, defined, 5-4

next hop, determining, 5-9

O

origin, defined, 5-2

P

parameters, IP
- IP Address, A-17
- Subnet Mask, A-17
- Transmit Bcast Addr, A-18

priority queuing, 6-10, A-30

publications
- ordering, xxiv

Q

Quality of Service (QoS), 6-2

R

resource manager, role in ST2 setup, 5-5

routing
- exploratory, 5-10
- IP-inherited, 5-9

S

SCMP (Stream Control Message Protocol), 5-4
ST2 parameters
  global
    Enable, A-19
    Tunneling Enable, A-20
    Tunnelling Capability, 5-13, A-19
  interface
    Accept Time Out, A-21
    Connect Retry, A-21
    Connect Time Out, A-21
    Disconnect Retry, A-22
    Disconnect Time Out, A-22
    Enable, 5-13, A-20
    Hello Retry, A-24
    Hello Time Out, A-24
    HID Change Retry, A-23
    HID Change Time Out, A-22
    IP Address, 5-13, A-20
    Refuse Retry, A-23
    Refuse Time Out, A-23
  neighbors
    Enable, A-24
    Hello Protocol, A-25
    Neighbor Priority Level, A-26
    Neighbor Type, A-25
    Next Hop IP Address, A-26
    Route Exploration Capability, A-25
ST2 protocol, defined, 6-2
ST2-capable, defined, 5-2
stream
  defined, 5-2
  setting up, 5-7
  shutting down, 5-12
Stream Control Message Protocol (SCMP), 5-4

T

target
  adding to a stream, 5-10
  defined, 5-2
technical response centers, xxv
tunnel, defined, 5-4

W

World Wide Web page, Bay Networks, xxv